Release Notes - Rev. C

OmniSwitch 6360, 6465, 6560(E), 6570M, 6860(E), 6860N, 6865, 6870, 6900, 9900

Release 8.10R2

These release notes accompany release 8.10R2. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Contents

Related Documentation

These release notes should be used in conjunction with OmniSwitch AOS Release 8 User Guides. The following are the titles of the user guides that apply to this release.

- OmniSwitch 6360 Hardware User Guide
- OmniSwitch 6465 Hardware User Guide
- OmniSwitch 6900 Hardware User Guide
- OmniSwitch 6560 Hardware User Guide
- OmniSwitch 6570M Hardware User Guide
- OmniSwitch 6860 Hardware User Guide
- OmniSwitch 6865 Hardware User Guide
- OmniSwitch 6870 Hardware User Guide
- OmniSwitch 9900 Hardware User Guide
- OmniSwitch AOS Release 8 CLI Reference Guide
- OmniSwitch AOS Release 8 Network Configuration Guide
- OmniSwitch AOS Release 8 Switch Management Guide
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
- OmniSwitch AOS Release 8 Specifications Guide
- OmniSwitch AOS Release 8 Transceivers Guide

System Specifications

Memory Specifications

The following are the standard shipped memory configurations. Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory.

Platform	SDRAM	Flash
OS6360	1GB	1GB
OS6465	1GB	1GB
OS6560(E)	2GB	2GB
OS6560-24X4/P24X4	1GB	1GB
OS6570M	2GB	8GB
OS6860(E)	2GB	2GB
OS6860N	4GB	16GB
OS6865	2GB	2GB
OS6870	8GB	32GB
OS6900-V72/C32	16GB	16GB
OS6900-X48C6/T48C6/X48C4E/T24C2/X24C2	8GB	32GB[1]
OS6900-V48C8/C32E	16GB[2]	64GB[1]
OS9900	16GB	2GB

1. Size of physical memory. Partitioned to 16GB flash memory.
2. Previous release notes incorrectly listed 8GB.

U-Boot and FPGA Specifications

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any U-Boot or FPGA upgrades but it's recommended to upgrade to the current version to address any known issues. Use the '**show hardware-info**' command to determine the current versions.

Switches not running the minimum version required should upgrade to the latest U-Boot or FPGA that is available with this AOS release software available from Service & Support.

Please refer to the Upgrade Instructions section at the end of these Release Notes for step-by-step instructions on upgrading your switch.

OmniSwitch 6360 – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6360-10	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.11	0.11 0.12[5]
OS6360-P10	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4]	0.11	0.11 0.12[5]

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.10.115.R01[6] 8.10.42.R02[6]		
OS6360-P10A (904324-90)	8.8.2.R03	8.8.2.R03 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.1	0.1 0.2[5]
OS6360-24	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.15	0.17[1] 0.20[3]
OS6360-P24	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.15	0.17[1] 0.20[3]
OS6360-P24X	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.12	0.12 0.13[5]
OS6360-PH24	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.12	0.12 0.13[5]
OS6360-48	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.15	0.17[1] 0.20[3]
OS6360-P48	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.15	0.17[1] 0.20[3]
OS6360-P48X	8.7.149.R02	8.7.30.R03[2] 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.12	0.12 0.13[5]
OS6360-PH48	8.8.114.R01	8.8.114.R01 8.9.85.R02[4] 8.10.115.R01[6] 8.10.42.R02[6]	0.12	0.12 0.13[5]

1. FPGA version 0.17 is REQUIRED to address issues CRAOS8X-26370 and CRAOS8X-25033.
2. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
3. Optional FPGA update for reduced fan speed at boot up.
4. Highly recommended to address NAND flash corruption issue CRAOS8X-35470. Also adds support for Gowin CPLD.
5. For switches currently shipping from the factory. No upgrade required for existing switches.
6. Addresses multiple power cycle issues. See FPGA / U-boot Upgrade Procedure.

OmniSwitch 6465 – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6465-P6	8.5.83.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.9.85.R02[5] 8.10.115.R01[6] 8.10.42.R02[6]	0.10	0.10
OS6465-P12	8.5.83.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.9.85.R02[5] 8.10.115.R01[6] 8.10.42.R02[6]	0.10	0.10
OS6465-P28	8.5.89.R02	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.9.85.R02[5] 8.10.115.R01[6] 8.10.42.R02[6]	0.5	0.7[1]
OS6465T-12	8.6.117.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.9.85.R02[5] 8.10.115.R01[6] 8.10.42.R02[6]	0.4	0.4
OS6465T-P12	8.6.117.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.9.85.R02[5] 8.10.115.R01[6] 8.10.42.R02[6]	0.4	0.4
OS6465-P12 (ENH-240)	8.8.33.R01	8.8.33.R01 8.9.85.R02[5] 8.10.115.R01[6] 8.10.42.R02[6]	0.5	0.5

1. FPGA version 0.7 is optional to address issue CRAOS8X-12042.
2. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.
3. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
4. Optional U-boot update to support boot from USB feature.
5. Highly recommended to address the NAND flash corruption issue CRAOS8X-35470.
6. Addresses multiple power cycle issues. See FPGA / U-boot Upgrade Procedure.

OmniSwitch 6560 – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-24Z24	8.5.22.R01	8.7.2.R02[3] 8.7.30.R03[7] 8.9.85.R02[9]	0.7	0.8[5] 0.9[9]

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.10.115.R01[10] 8.10.42.R02[10]		
OS6560-P24Z24	8.4.1.23.R02	8.7.2.R02[3] 8.7.30.R03[7] 8.9.85.R02[9] 8.10.115.R01[10] 8.10.42.R02[10]	0.6	0.7[1] 0.8[5] 0.9[9]
OS6560-24Z8	8.5.22.R01	8.7.2.R02[3] 8.7.30.R03[7] 8.9.85.R02[9] 8.10.115.R01[10] 8.10.42.R02[10]	0.7	0.8[5] 0.9[9]
OS6560-P24Z8	8.4.1.23.R02	8.7.2.R02[3] 8.7.30.R03[7] 8.9.85.R02[9] 8.10.115.R01[10] 8.10.42.R02[10]	0.6	0.7[1] 0.8[5] 0.9[9]
OS6560-24X4	8.5.89.R02	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8] 8.10.115.R01[10] 8.10.42.R02[10]	0.4	0.4
OS6560-P24X4	8.5.89.R02	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8] 8.10.115.R01[10] 8.10.42.R02[10]	0.4	0.4
OS6560-P48Z16 (903954-90)	8.4.1.23.R02	8.7.2.R02[3] 8.7.30.R03[7] 8.9.85.R02[9] 8.10.115.R01[10] 8.10.42.R02[10]	0.6	0.7[1] 0.8[5] 0.9[9]
OS6560-P48Z16 (all other PNs)	8.5.97.R04	8.7.2.R02[3] 8.7.30.R03[7] 8.9.85.R02[9] 8.10.115.R01[10] 8.10.42.R02[10]	0.3	0.6[2] 0.7[6]
OS6560-48X4	8.5.97.R04	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8] 8.10.115.R01[10] 8.10.42.R02[10]	0.4	0.7[2] 0.8[6]
OS6560-P48X4	8.5.97.R04	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8] 8.10.115.R01[10] 8.10.42.R02[10]	0.4	0.7[2] 0.8[6]

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6560-X10	8.5.97.R04	8.7.2.R02[4] 8.7.30.R03[7] 8.9.85.R02[8] 8.10.115.R01[10] 8.10.42.R02[10]	0.5	0.8[2]
OS6560E-P24Z8	8.9.85.R02	8.9.85.R02 8.10.115.R01[10] 8.10.42.R02[10]	0.9	0.9
OS6560E-P48Z16	8.9.85.R02	8.9.85.R02 8.10.115.R01[10] 8.10.42.R02[10]	0.7	0.7

1. FPGA version 0.7 is optional to address issue CRAOS8X-7207.
2. FPGA versions are optional to address issue CRAOS8X-16452.
3. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.
4. U-boot 8.7.2.R02 is optional to address UBIFS error issues CRAOS8X-4813/13440.
5. FPGA version 0.8 is optional to address issue CRAOS8X-22857.
6. FPGA versions 0.7 and 0.8 are optional to support 1588v2.
7. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
8. Highly recommended to address the NAND flash corruption issue CRAOS8X-35470.
9. Ships from factory. No upgrade required, there are no functional changes in this U-boot version for these models.
10. Addresses multiple power cycle issues. See FPGA / U-boot Upgrade Procedure.

OmniSwitch 6570M - AOS Release 8.10.105.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6570M-12	8.9.25.R02	8.9.25.R02 8.9.92.R02[1] 8.9.139.R03[3] 8.9.70.R04[4] 8.10.115.R01[5] 8.10.42.R02[5]	0.11	0.11
OS6570M-12D	8.9.25.R02	8.9.25.R02 8.9.92.R02[1] 8.9.139.R03[3] 8.9.70.R04[4] 8.10.115.R01[5] 8.10.42.R02[5]	0.11	0.11
OS6570M-U28	8.9.25.R02	8.9.25.R02 8.9.92.R02[1] 8.9.139.R03[3] 8.9.70.R04[4] 8.10.115.R01[5] 8.10.42.R02[5]	0.11	0.11 0.12[2]

1. Adds support for Gowin CPLD.
2. Addresses power supply interrupt issue.
3. Addresses CRAOS8X-40924 for disabling U-boot access.
4. Adds support for signed AOS images.
5. Addresses multiple power cycle issues. See FPGA / U-boot Upgrade Procedure.

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
Note: U-boot version 8.9.70.R04 and above supports AOS signed images only (8.9R4 and above). To use AOS releases prior to 8.9R4, before downgrading the AOS image the u-boot must be downgraded to a version earlier than 8.9.70.R04.				

OmniSwitch 6860(E) – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6860/OS6860E (except U28/P24Z8)	8.1.1.70.R01	8.7.30.R03[2] 8.10.115.R01[3] 8.10.42.R02[3]	0.9	0.10[1]
OS6860E-U28	8.1.1.70.R01	8.7.30.R03[2] 8.10.115.R01[3] 8.10.42.R02[3]	0.20	0.20
OS6860E-P24Z8	8.4.1.17.R01	8.7.30.R03[2] 8.10.115.R01[3] 8.10.42.R02[3]	0.5	0.7[1]
1. FPGA versions .7 and .10 are optional on the PoE models for the fast and perpetual PoE feature support. 2. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access. 3. Addresses multiple power cycle issues. See FPGA / U-boot Upgrade Procedure.				

OmniSwitch 6860N – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6860N-U28	2019.05.00.10	2019.05.00.11	12	12
OS6860N-P48Z	2019.05.00.10	2019.05.00.11	12	13[1]
OS6860N-P48M	2019.05.00.10	2019.05.00.11	11	12[1]
O6860N-P24M	2019.05.00.11	2019.05.00.11	2	3[1]
OS6860N-P24Z	2019.05.00.11	2019.05.00.11	2	3[1]
1. Addresses CRAOS8X-29731/30471 – OS6860N power supply issue. **Note**: These models use the **Uosn.img** image file.				

OmniSwitch 6865 – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
OS6865-P16X	8.3.1.125.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.10.115.R01[5] 8.10.42.R02[5]	0.20	0.25[1]
OS6865-U12X	8.4.1.17.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4]	0.23	0.25[1]

Hardware	Minimum U-Boot	Current U-Boot	Minimum FPGA	Current FPGA
		8.10.115.R01[5] 8.10.42.R02[5]		
OS6865-U28X	8.4.1.17.R01	8.7.2.R02[2] 8.7.30.R03[3] 8.8.33.R01[4] 8.10.115.R01[5] 8.10.42.R02[5]	0.11	0.14[1]

1. FPGA versions 0.25 and 0.14 are optional for the fast and perpetual PoE feature support.
2. U-boot 8.7.2.R02 is optional to address eUSB issue CRAOS8X-13819.
3. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
4. Optional U-boot update to support boot from USB feature.
5. Addresses multiple power cycle issues. See FPGA / U-boot Upgrade Procedure.

Note: CRAOS8X-4150 for the OS6865-U28X was fixed with FPGA version 0.12 and higher.

OmniSwitch 6870 – AOS Release 8.10.105.R02 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6870-24	2019.05.00.12	2019.05.00.12	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04
OS6870-P24M	2019.05.00.12	2019.05.00.12	CPLD - 0.09 CPLD (LED) - 0.07 CPLD (CPU) - 0.04	CPLD - 0.09 CPLD (LED) - 0.07 CPLD (CPU) - 0.04
OS6870-P24Z	2019.05.00.12	2019.05.00.12	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04
OS6870-48	2019.05.00.12	2019.05.00.12	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04	CPLD - 0.09 CPLD (LED) - 0.08 CPLD (CPU) - 0.04
OS6870-P48M	2019.05.00.12	2019.05.00.12	CPLD - 0.11 CPLD (LED) - 0.09 CPLD (CPU) - 0.04	CPLD - 0.011 CPLD (LED) - 0.09 CPLD (CPU) - 0.04
OS6870-P48Z	2019.05.00.12	2019.05.00.12	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04	CPLD - 0.07 CPLD (LED) - 0.06 CPLD (CPU) - 0.04
OS6870-V12	2019.05.00.12	2019.05.00.12	CPLD - 0.10 CPLD (LED) - 0.07 CPLD (CPU) - 0.04	CPLD - 0.10 CPLD (LED) - 0.07 CPLD (CPU) - 0.04

OmniSwitch 6900 - AOS Release 8.10.105.R02 (GA)

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-V72	2017.08.00.01	2017.08.00.01	CPLD 1 – 5 CPLD 2 - 6 CPLD 3 – 8	CPLD 1 – 5 CPLD 2 - 6 CPLD 3 – 8
OS6900-C32	2016.08.00.03	2018.11.00.02	CPLD 1 – 10 CPLD 2 – 11 CPLD 3 – 11	CPLD 1 – 10 CPLD 2 – 11 CPLD 3 – 11

Hardware	Minimum ONIE	Current ONIE	Minimum CPLD	Current CPLD
OS6900-C32E	2020.02.00.01	2020.02.00.01	CPLD 1 – 13 CPLD 2 – 9 CPLD 3 – 9	CPLD 1 – 13 CPLD 2 – 9 CPLD 3 – 9
OS6900-X48C6	2019.08.00.01	2019.08.00.01	CPLD 1 – 2 CPLD 2 - 2 CPLD 3 – 2 CPU CPLD – N/A	CPLD 1 – 3 CPLD 2 - 2 CPLD 3 – 2 CPU CPLD – 2.14[1]
OS6900-T48C6	2019.08.00.01	2019.08.00.01	CPLD 1 – 2 CPLD 2 – 2 CPLD 3 – 4 CPU CPLD – N/A	CPLD 1 – 3 CPLD 2 – 2 CPLD 3 – 4 CPU CPLD – 2.14[1]
OS6900-X48C4E	2019.05.00.10	2019.05.00.10	CPLD 1 – 3 CPLD 2 - 2 CPLD 3 – 3 CPU CPLD – N/A	CPLD 1 – 3 CPLD 2 - 2 CPLD 3 – 3 CPU CPLD – 2.14[1] CPU CPLD – 2.15[2]
OS6900-V48C8	2020.02.00.01	2020.02.00.01	CPLD 1 – 2 CPLD 2 - 3 CPLD 3 – 2	CPLD 1 – 2 CPLD 2 - 3 CPLD 3 – 2
OS6900-T24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0	CPLD 1 - 2.0 CPLD 2 - 2.0 CPLD CPU - 6.0
OS6900-X24C2	2019.08.00.03	2019.08.00.03	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0	CPLD 1 - 6.0 CPLD 2 - 6.0 CPLD CPU - 6.0

1. Optional CPU CPLD update to address CRAOS8X-30098.
2. Required CPLD update to address CRAOS8X-43968 (Hardware revision 6 only).

OmniSwitch 9900 – AOS Release 8.10.106.R02 (GA)

Hardware	Minimum Coreboot-Uboot	Current Coreboot-Uboot	Minimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-CMM	8.3.1.103.R01	8.3.1.103.R01 8.7.30.R03[1] 8.8.152.R01	2.3.0	2.3.0	0.8
OS99-CMM2	8.9.183.R03	8.9.183.R03	1.4.0	1.4.0	1.2.0
OS9907-CFM	-	-	-	-	-
OS9907-CFM2	-	-	-	-	-
OS9912-CFM	-	-	-	-	-
OS99-GNI-48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	1.2.4	1.2.4 1.2.5[2]	0.9
OS99-GNI-P48	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	1.2.4	1.2.4 1.2.5[2]	0.9

Hardware	Minimum Coreboot-Uboot	Current Coreboot-Uboot	Minimun Control FPGA	Current Control FPGA	Minimum/ Current Power FPGA
OS99-XNI-48 (903753-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	1.3.0	1.3.0 1.5.0[2]	0.6
OS99-XNI-48 (904049-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01[2]	1.4.0	1.4.0 1.5.0[2]	0.7
OS99-XNI-U48 (903723-90)	8.3.1.103.R01	8.3.1.103.R01 8.8.152.R01[2]	2.9.0	2.9.0 2.11.0[2]	0.8
OS99-XNI-U48 (904047-90)	8.6.261.R01	8.6.261.R01 8.8.152.R01[2]	2.10.0	2.10.0 2.11.0[2] 2.12.0[3]	0.8
OS99-GNI-U48	8.4.1.166.R01	8.4.1.166.R01 8.8.152.R01[2]	1.6.0	1.6.0 1.7.0[2] 1.8.0[3]	0.2
OS99-CNI-U8	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01[2]	1.7	1.7 1.9[2] 1.10[3]	N/A
OS99-XNI-P48Z16[4]	8.4.1.20.R03	8.4.1.20.R03 8.8.152.R01[2]	1.4	1.4 1.6[2]	0.7
OS99-XNI-U24	8.5.76.R04	8.6.261.R01 8.8.152.R01[2]	1.0	2.9.0 2.11.0[2] 2.12.0[3]	0.8
OS99-XNI-P24Z8[4]	8.5.76.R04	8.6.261.R01 8.8.152.R01[2]	1.1	1.4.0 1.6.0[2]	0.7
OS99-XNI-U12Q[4]	8.6.117.R01	8.6.117.R01 8.8.152.R01[2]	1.6.0	1.5.0 1.6.0[2]	N/A
OS99-XNI-UP24Q2[4]	8.6.117.R01	8.6.117.R01 8.8.152.R01[2]	1.5.0	1.5.0 1.6.0[2]	N/A
OS99-CNI-U20	8.9.183.R03	8.9.183.R03	1.2.0	1.2.0	0.4

1. Optional U-boot update for CRAOS8X-24464, ability to disable/authenticate U-boot access.
2. Optional U-boot/FPGA update for CMM2 and OS9912 compatibility.
3. Optional FPGA upgrade to address CRAOS8X-43592: 1G/10G SFP not recognized.
4. Not currently supported in an OS9912 chassis.

Note: Existing OS9900 NIs that are to be used with a CMM2 or in an OS9912 chassis must first have the Uboot and FPGA upgraded before using them with a CMM2 or inserting them into an OS9912 chassis. See footnote #2.

[IMPORTANT] *MUST READ*: AOS Release 8.10R2 Prerequisites and Deployment Information

General Information

- Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.
- Please refer to the Feature Matrix in Appendix A for detailed information on supported features for each platform.
- Prior to upgrading please refer to Appendix D for important best practices, prerequisites, and step-by-step instructions.
- Some switches may ship from the factory with a diag.img file. This file is for internal switch diagnostic purposes only and can be safely removed.
  Switches that ship from the factory will have the Running Configuration set to the /flash/working directory upon the first boot up. By default, the automatic VC feature will run and the vcboot.cfg and vcsetup.cfg files will be created in the /flash/working directory but not in the /flash/certified directory which results in the Running Configuration not being certified. This will result in the Running Configuration being set to the /flash/certified directory on the next reboot. Additionally, on the next reboot the switch will no longer be in the factory default mode and will have a chassis-id of 1 which could cause a duplicate chassis-id issue if the switch is part of a VC. To set the switch back to the factory defaults on the next reboot perform the following:

  ```
  -> rm /flash/working/vcboot.cfg
  -> rm /flash/working/vcsetup.cfg
  -> rm /flash/certified/vcboot.cfg
  -> rm /flash/certified/vcsetup.cfg
  ```

- The OS6560-P48Z16 (903954-90) supports link aggregation only on the 1G/2.5G multigig and 10G ports (33-52). The 1G ports (ports 1-32) do not support link aggregation (CRAOSX-1766). Linkagg configuration on unsupported ports in 85R1/841R03 config file will be removed internally from software during upgrade reboot. Oversized frames will not be dropped on ingress of ports 1-32 (CRAOS8X-20939).

  Note: OS6560-P48Z16 (all other PNs) - This is a new version of the OS6560-P48Z16 which does not have the limitations mentioned above. The model number (OS6560-P48Z16) remains the same for both versions, only the part number can be used to differentiate between the versions.

- Improved Convergence Performance
  Faster convergence times can be achieved on models with SFP, SFP+, QSFP+, and QSFP28 ports with fiber transceivers.

  Exceptions:
  - Copper ports or ports with copper transceivers do not support faster convergence.
  - OS6865-P16X and OS6865-U12X ports 3 and 4 do not support faster convergence.
  - VFL ports do not support faster convergence.
  - Splitter ports (i.e. 4X10G or 4X25G) do not support faster convergence.
  - OS6570M-12/12D ports 9 and 10 do not support fast convergence.

- MACsec Licensing Requirement
  Beginning in 8.6R1 the MACsec feature requires a site license, this license can be generated free of cost. After upgrading, the feature will be disabled until a license is installed. There is no reboot required after applying the license.

- SHA-1 Algorithm - Chosen-prefix attacks against the SHA-1 algorithm are becoming easier for an attacker[1]. For this reason, we have disabled the "ssh-rsa" public key signature algorithm by default. The better alternatives include:

- The RFC8332 RSA SHA-2 signature algorithms rsa-sha2-256/512. These algorithms have the advantage of using the same key type as "ssh-rsa" but use the safer SHA-2 hash algorithms. RSA SHA-2 is enabled in AOS.
- The RFC5656 ECDSA algorithms: ecdsa-sha2-nistp256/384/521. These algorithms are supported in AOS by default.

To check whether a server is using the weak ssh-rsa public key algorithm, for host authentication, try to connect to it after disabling the ssh-rsa algorithm from ssh(1)'s allowed list using the command below:

```
-> ssh strong-hmacs enable
```

If the host key verification fails and no other supported host key types are available, the server software on that host should be upgraded.

1. "SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust" Leurent, G and Peyrin, T (2020) https://eprint.iacr.org/2020/014.pdf

- With the continuous goal of preserving the environment in addition to the AOS software being preloaded on the switch and available on the Business Portal, we have begun removing the software access card previously included in the switch ship kit. For additional information or if in need of special assistance, please contact Service & Support.

Deprecated Features / Functionality Changes

The following table lists deprecated features and key functionality changes by release.

AOS Release 8.5R4
EVB - Beginning in 8.5R4, support for EVB is being removed. Any switches with an EVB configuration cannot be upgraded to 8.5R4 or above.
NTP - Beginning with AOS Release 8.5R4, OmniSwitches will not synchronize with an unsynchronized NTP server (stratum 16), as per the RFC standard. Existing installations where OmniSwitches are synchronizing from another OmniSwitch, or any other NTP server which is not synchronized with a valid NTP server, will not be able to synchronize their clocks. The following NTP commands have been deprecated: - ntp server synchronized - ntp server unsynchronized
AOS Release 8.6R1
DHCPv6 Guard - Configuration via an IPv6 interface name is deprecated in 8.6.R1. Commands entered using the CLI must use the new 'ipv6 dhcp guard vlan vlan-id' format of the command. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
IP Helper - The 'ip helper' commands have been deprecated in 8.6R1 and replaced with 'ip dhcp relay'. The old format will still be accepted if present in a vcboot.cfg to preserve backwards compatibility.
SAA - The vlan-priority and drop-eligible parameters have been deprecated from all SAA commands beginning in 8.6R1.
MACsec is now supported on ports 33-48 of the 6560-(P)48X4. CRAOS8X-7910 was resolved in 8.6R1.
AOS Release 8.6R2
Distributed ARP - Beginning 8.6R2 distributed ARP is no longer supported.
WRED - Beginning in 8.6R2 WRED is no longer supported.
QoS - Beginning in 8.6R2 the 'qos dscp-table' command is no longer supported.
NTP - The ntp parameter for the 'ip service source-ip' command was deprecated in 8.5R4. Support has been added back in 8.6R2.

AOS Release 8.7R1
MACsec - Static mode is not supported on OS6860N.
Transceivers - Beginning in AOS release 8.7R1 an error message will be displayed when the unsupported QSFP-4X25G-C transceiver is inserted on an OS99-CNI-U8 module.
SPB - Beginning in 8.7.R01 the default number of BVLANs created via Auto Fabric is reduced from 16 to 4. This new default value is only applicable to factory default switches running 8.7R1 with no vcboot.cfg file. Upgrading to 8.7.R1 will not change the number of configured BVLANs in an existing configuration. See Appendix C for additional information.
AOS Release 8.7R2
There are new default user password polices being implemented in 8.7R2. This change does not affect existing users. - cannot-contain-username: enable - min-uppercase: 1 - min-lowercase: 1 - min-digit: 1 - min-nonalpha: 1
The OmniSwitch 6360 does not contain a real-time clock. - It is recommended to use NTP to ensure time synchronization on OS6360s. - When the switch is reset, the switch will boot up from an approximation of the last known good time. - When the switch is powered off it cannot detect the time left in the powered off state. When it boots up it will have the same time as when the switch was last powered off.
AOS Release 8.7R3
The Kerberos Snooping is not supported in bridge mode in this release.
AOS Release 8.8R1
Unsupported commands (Part of AOS 88R1 but not supported) - mrp interconnect - show mrp interconnect - clear mrp interconnect
A software check was added in AOS releases 8.7R1, 8.7R2, and 8.7R3 restricting the use of the affected power supplies below while awaiting certification on the OS6560. This check was removed in 8.8R1 after the power supplies were certified resulting in the minimum AOS version 8.8R1 requirement. **OS6560-BP-PH** - This OS6560 600W power supply, OS6560-BP-PH (904072-90), requires a minimum AOS version of 8.8R1. **OS6560-BP-PX** - This OS6560 920W power supply, OS6560-BP-BX (904073-90), requires a minimum AOS version of 8.8R1. Refer to the OmniSwitch 6560 Hardware Guide for additional power supply information.
AOS Release 8.8R2
The French language support is being removed from WebView to help reduce package size. If the default language is French it will default to English after upgrade.
AOS Release 8.9R1
Metro License Features – Some Metro features are now licensed on the OS6560 beginning in 8.9R1. See Metro License for information on re-enabling them after upgrading to 8.9R1.
AOS Release 8.9R4
OmniSwitch 6570 signed AOS image support with proper u-boot was added.
AOS Release 8.10R1
CRAOS8X-46556 (CVE-2024-6387) fix has been implemented by default in 8.10R1. See Appendix K: Fixed CVEs.
AOS Release 8.10R2
- Support for OVSDB removed.
- The administrative state for the automatic fabric feature is disabled by default.

- The U-boot version on the OS6570M models shipping from the factory is 8.10.42.R02. This U-boot version supports signed AOS images only (8.9R4 and above). To use AOS releases prior to 8.9R4 the u-boot version must first be downgraded to a version below 8.9.70.R04 before downgrading AOS.

Licensed Features

The table below lists the CAPEX licensed features in this release and whether or not a license is required for the various models. Refer to the licensing portal.

	Data Center License Required
	OmniSwitch
Licensed Features	
DCB (PFC,ETS,DCBx)	Not Supported
FIP Snooping	Not Supported
FCoE VxLAN	Not Supported

	Feature/Performance License Required								
	OS6360	OS6465	OS6560	OS6570M	OS6860	OS6860N	OS6870	OS6900	OS9900
Licensed Features									
MACsec (OS-SW-MACSEC)	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]	Yes
10G Support (OS6560-SW-PERF)	N/A	N/A	Yes[1]	N/A	N/A	N/A	N/A	N/A	N/A
10G Support (OS6360-SW-PERF)	Yes[2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10G Support (OS6570-SW-PERF4)	N/A	N/A	N/A	Yes[4]	N/A	N/A	N/A	N/A	N/A
MPLS Support (OS####-MPLS-#)	N/A	N/A	N/A	N/A	N/A	Yes	N/A	Yes	N/A
50G Support (OS6870-SW-PERF)	N/A	N/A	N/A	N/A	N/A	N/A	Yes[5]	N/A	N/A

1. Performance software license is optional allowing ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4) to operate at 10G speed. Ports support 1G by default.
2. Performance software license is optional allowing the 2 RJ45/SFP+ combo ports (25/26 or 49/50) of the OS6360-PH24 or OS6360-PH48 models to operate at 10G speed. Ports support 1G by default.
3. MACsec is supported on the OS6900-X48C4E.
4. Performance software license is optional allowing the OS6570M-U28 ports 25-28 to operate at 10G speed. Ports support 1G by default.
5. Performance software license is optional allowing the OS6870-LNI-U6 ports to operate at 50G speed. Ports support up to 25G by default.

	Metro License Required
	OmniSwitch 6560
Licensed Features	
CPE Test Head	Yes
PPPoE-IA	Yes
Ethernet OAM	Yes
SAA	Yes
Link OAM	Yes
VLAN Stacking	Yes
DPA	Yes
Hardware Loopback	Yes
IPMVLAN	Yes
Note: Starting in 8.9R1 the features above require a Metro license.	

	Advanced Routing License Required	
	OmniSwitch 6570M	OmniSwitch 6560
Licensed Features		
OSPFv2 and OSPFv3	Yes	Yes (Up to 2 Areas)
PIM Multicast Routing (IPv4 & IPv6)	Yes	Yes
Multiple VRFs	Yes	Not Supported
ISIS (IPv4 and IPv6)	Yes	Not Supported
GRE Tunneling	Yes	Not Supported
IP-IP Tunneling	Yes	Not Supported
Route Redistribution	Yes	Yes
VRF Route Leaking	Yes	Not Supported
BGP	Yes	Not Supported
Note: The table above lists the features supported with the Advanced Routing license.		

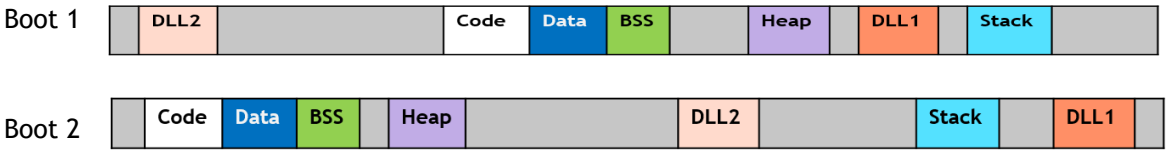
ALE Secure Diversified Code

Alcatel-Lucent Enterprise provides network equipment that is hardened in conjunction with an independent 3rd party organization. ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification to prevent exploitation. OmniSwitch products can also be delivered that are TAA Country of Origin USA compliant with AOS software loaded from US based servers onto the OmniSwitch in a US factory. This is the default operation of AOS, there is no charge or additional licensing required.

ALE secure diversified code employs multiple techniques to identify vulnerabilities such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third party code.

Software Diversification

Software diversification rearranges the memory map of the executable program so that various instances of the same software, while functionally identical, are arranged differently in memory. In AOS 8.6.R01, ALE has adopted address system layout randomization(ASLR) as a standard feature. ASLR results in a unique memory layout of the running software each time the OmniSwitch reboots to impede or prevent software exploitation. ASLR is depicted below showing that two different system boots results in two different memory layouts for code segments, data segments, dynamic libraries, etc.



Please contact customer support for additional information.

New / Updated Hardware Support and Guidelines

OmniSwitch 6870-24
Fixed-configuration chassis in a 1U form factor with:
- 24 - 10/100/1000 Base-T RJ-45 Ports
- 4 - 1G/10G/25G SFP28 Uplink Ports
- 2 - 40G/100G QSFP28 VFL Ports
- USB port
- RJ-45 console port

OmniSwitch 6870-P24M
Modular chassis in a 1U form factor with:
- 24 - 100M/1G/2.5G/5G/10G Multi-gigabit RJ-45 802.3bt PoE (95W) Ports
- 2 - 40G/100G/200G QSFP56 VFL Ports
- 1 - Uplink Module Slot
- USB port
- RJ-45 console port

OmniSwitch 6870-P24Z
Fixed-configuration chassis in a 1U form factor with:
- 24 - 100M/1G/2.5G Multi-gigabit RJ-45 802.3bt PoE (60W) Ports
- 6 - 1G/10G/25G SFP28 Uplink Ports
- 2 - 40G/100G QSFP28 VFL Ports
- USB port
- RJ-45 console port

OmniSwitch 6870-48
Fixed-configuration chassis in a 1U form factor with:
- 48 - 10/100/1000 Base-T RJ-45 Ports
- 4 - 1G/10G/25G SFP28 Uplink Ports
- 2 - 40G/100G QSFP28 VFL Ports
- USB port
- RJ-45 console port

OmniSwitch 6870-P48M
Modular chassis in a 1U form factor with:
- 48 - 100M/1G/2.5G/5G Multi-gigabit RJ-45 802.3bt PoE (95W) Ports
- 2 - 40G/100G/200G QSFP56 VFL Ports
- 1 - Uplink Module Slot
- USB port
- RJ-45 console port

OmniSwitch 6870-P48Z
Fixed-configuration chassis in a 1U form factor with:
- 48 - 100M/1G/2.5G Multi-Gig RJ-45 802.3bt PoE (60W) Ports
- 6 - 1G/10G/25G SFP28 Uplinks
- 2 - 40G/100G/200G QSFP56 VFL Ports
- USB port
- RJ-45 console port

OmniSwitch 6870-V12
Fixed-configuration chassis in a 1U form factor with:

- 12 - 1G/10G/25G SFP28 Ports
- 2 - 40G/100G/200G QSFP56 VFL Ports
- 1 - Uplink Module Slot
- USB port
- RJ-45 console port

OS6870-CNI-U2
Uplink module with:

- 2 - 40G/100G QSFP28 VFL Ports

OS6870-LNI-U6
Uplink module with:

- 6 - 1G/10G/25G/50G SFP56 Uplink Ports (OS6870-SW-PERF license required for 50G speeds)

OS6870-BP
250W AC system power supply.

OS6870-BP-D
250W DC system power supply.

OS6870-BPH
550W AC system power supply.

OS6870-BPPH
600W AC system and PoE power supply.

OS6870-BPPX
1200W AC system and PoE power supply.

OS6870-BPXL
2000W AC system and PoE power supply.

SFP-50G-SR - 50-Gigabit optical transceiver (SFP56). Supports multi-mode fiber. Typical reach 100m. LC connector.

SFP-50G-FR - 50-Gigabit optical transceiver (SFP56). Supports single-mode fiber. Typical reach 2km. LC connector.

SFP-50G-LR - 50-Gigabit optical transceiver (SFP56). Supports single-mode fiber. Typical reach 10km. LC connector.

SFP-50G-C1M/C3M/C50CM
50-Gigabit direct attach cable (QSFP56). Available in 1m, 3m, and 50cm lengths.

QSFP-200G-SR4
200-Gigabit optical transceiver (QSFP56). Supports multi-mode fiber. Typical reach 100m. MPO-12 connector.

QSFP-200G-FR4
200-Gigabit optical transceiver (QSFP56). Supports single-mode fiber. Typical reach 2km. LC connector.

QSFP-200G-A20M
200-Gigabit direct attached active optical cable. (QSFP56). Supports single-mode fiber. Typical reach 20m.

QSFP-200G-C1M/3M/C50CM
200-Gigabit direct attach cable (QSFP56). Available in 1m, 3m, and 50cm lengths.

OS9907 Chassis OS99-CMM2 Support
8.10R2 adds support for using the OS99-CMM2 in the OS9907 chassis. With the introduction of the CMM2 there are multiple possible CMM/CMM2/CFM/CFM2 combinations on an OS9907 chassis. Not all combinations are supported. Use the table below for the supported combinations for an OS9907 chassis.

CMM Combination	CFM Combination	Support
CMM + CMM	CFM + CFM	Supported
CMM + CMM	CFM2 + CFM2	Supported
CMM + CMM	CFM + CFM2	Not Supported
CMM2 + CMM2	CFM2 + CFM2	Supported
CMM2 + CMM2	CFM + CFM	Not Supported
CMM2 + CMM2	CFM + CFM2	Not Supported
CMM + CMM2	NA	Not Supported

OS9907 VC Configuration Support
The combinations below support an OS9907 VC-of-2 configuration.

Chassis 1	Chassis 2	Support
CMM + CFM	CMM + CFM	Supported
CMM + CFM2	CMM + CFM2	Supported
CMM2 + CFM2	CMM2 + CFM2	Supported
All other combination		Not Supported

8.10R2 New Feature and Enhancements

The following software features are being introduced in this release, subject to the feature exceptions and problem reports described later in these release notes.

Summary Table

Feature	OmniSwitch Platform
Management Features	
Switch Reload Enhancement – Certify On Reboot	6465,6560,6570M, 6860, 6865, 6870
ARP Scalability Support	6870/9907
ARP Scalability Edge-router Mode	6870/9900
50G License Support	6870
Auto-Fabric Administrative State Disabled by Default	All
Lightning Configuration Updates	6360
Alert for Scheduled Reboot	All
Password Expiration to 365 Days	All
Layer 3 Features	
DHCPv6 Guard and Snooping on a Service	6860N, 6870, 6900
Discovering PREF64 in Router Advertisements	All
EMP IPv6 VRF support	6570M, 6860, 6860N, 6865, 6870, 6900, 9900
DNS IPv6 Configurable Per Network	All
Service Features	
EVPN Enhancements	6900 (except V72/C32)
EVPN- BGP Route reflectors: Intra domain(I-BGP)	6900 (except V72/C32)
VPLS on OS6900	6900 (except V72/C32)
MPLS OAM LSP Ping and Traceroute Support	6860N, 6900 (except V72/C32)
Virtual Private Wire Service (VPWS) Support	6860N, 6900 (except V72/C32)
Transparent Bridging	6870
QoS/Security Features	
MACsec Support	6570M, 6870,9900
Option to Disable 'exit-on-fail' for AAA Authentication	All
Kerberos-snooping on 6870 (VLAN/Service-domain)	6870
IEEE Drop Enhancement	6465, 6560, 6570M
Other Features	
Precison Time Protocol (PTP) – End-to-End Support	6860N, 6900-V48
Storm Control Handling of Unknown Unicast Traffic with Action as Shutdown	6870
Route Advertisement Filtering (RAF) and Local Proxy Neighbor Discover (LPND) support.	6870

Feature	OmniSwitch Platform
TCAM Profiles	6870

Management Features

Switch Reload Enhancement – Certify on Reboot

This feature loads and certifies the images in the ***working*** directory on the next reload or power cycle. It can be used after new image files are copied to the ***working*** directory to force the switch to reload from the ***working*** directory on the next reboot without having to use the **reload from working** command.

- This feature is supported only if the RUNNING directory is the ***working*** directory. If RUNNING directory is not ***working*** this feature will return an error when entered.
- After the command is entered the switch will continue to operate from the current RUNNING directory using the currently loaded images until the switch is rebooted.
- On the next reboot, either a manual reload or a power cycle, the switch is forced to boot from the ***working*** directory using the new images. Any commands attempting to reboot the switch from another directory are ignored.
- If the reboot fails with the new images in the ***working*** directory, the switch will boot from the ***certified*** directory.
- The **copy flash-synchro** operation to synchronize the ***certified*** directory with the new images will be automatically performed after the reboot is complete.
- This feature will remain enabled across reboots. Use the **no certify-on-reboot** command to disable.
- This feature is supported only on a VC-of-1. After enabling, no other units will be allowed to join the VC-of-1.
- After enabling the CLI **write memory flash-sync** will only copy the configuration files to the ***certified*** directory, not image files.
- Use the **show reload** command to show the status of certify-on-reboot.

The following CLI commands are associated with this feature:

- [no] certify-on-reboot
- show reload

ARP Scalability Support

The OS6870 supports 24K ARP entries in the default **switch** mode.

The **edge-router** mode increases the number of ARPs supported on the OS99-CNI-U20 and OS6870 to 64K. Edge-router mode is supported on the platforms below. An OS9900 with any modules others than an OS99-CMM2 and OS99-CNI-U20 cannot have edge-router mode enabled.

- OS9907 with OS99-CMM2 and OS99-CNI-U20
- OS9912 with OS99-CMM2 and OS99-CNI-U20
- OS6870

The following CLI commands are associated with this feature:

- capability profile edge-router
- show capability profile

50G License Support

The OS6870-LNI-U6 module supports 6 x 25G port speeds by default. The OS6870-SW-PERF license allows the OS6870-LNI-U6 to support 50G speeds. The license is installed using the Site Local Licensing Server (SILOS). A demo license is activated upon insertion of a 50G transceiver which will expire in 15 days if a permanent license is not installed. The demo period will be extended to 30 days if the license client makes a connection to the license server.

The following CLI commands are associated with this feature:

- license server
- license server apply
- license server remove
- license client
- license client remove
- show license-server
- show license-server info
- show license-server usage
- show license-client info
- ip interface Loopback0 address

Auto-Fabric Administrative State Disabled by Default

Beginning in 8.10R2 the administrative state for the automatic fabric feature will be disabled by default.

The following CLI commands are associated with this feature:

- auto-fabric admin-state {enable | disable}

Lightning Configuration Updates

To help simplify the wizard the auto-fabric, Bluetooth, and memory threshold fields have been removed. An option to include an IP address for an SNMP station and a warning to reload from the Working directory before proceeding if the switch initially booted from the Certified directory. Additionally, a text box has been added that can be used to include CLI commands for custom changes.

Alert for Scheduled Reboot

This enhancement will display a message after the banner to alert the user if there is a pending reboot scheduled.

The following CLI commands are associated with this feature:

- reload {from | all}
- reload cancel
- show reload

Allow Password Expiration Beyond 150 Days

The range for the number of days before locally configured user passwords will expire can now be configured from 1 to 365 days. This applies for both default password expiration and user password expiration.

The following CLI commands are associated with this feature:

- user password-expiration {*day* | disable}

Layer 3 Features

DHCPv6 Guard and Snooping on a Service

The functionality of DHCPv6 client Guard, DHCPv6 server Guard and DHCPv6 Snooping is extended to service domain.

The following CLI commands are associated with this feature:

- ipv6 dhcp guard service
- dhcpv6-snooping service admin-state
- dhcpv6-snooping binding service
- show dhcpv6-snooping
- show dhcpv6-snooping interfaces
- show dhcpv6-snooping binding
- show ipv6 dhcp guard

Discovering PREF64 in Router Advertisements

OmniSwitch must be able to seamless communicate between IPv6-only and IPv4-only devices. This is achieved by discovering PREF64 in Router Advertisements (RA) which serves as a means of informing IPv6 hosts about the preferred IPv6 prefix to use for translating IPv4 addresses to IPv6 addresses in NAT64 networks. The switch uses the RA to advertise the NAT64 prefix which can be used by the NAT64 device in the network.

The following CLI commands are associated with this feature:

- ipv6 interface <ifname> [ra-nat64-prefix <ip6addr/preflen> | no ra-nat64-prefix]

EMP IPv6 VRF Support

The OmniSwitch supports creating of chassis EMP and virtual chassis EMP. The EMP interface is supported only on default VRF.

The following CLI commands are associated with this feature:

- ipv6 emp-interface [local-chassis <chassis-id> I vc-master] [address <address>/<prefix-length>]
- no ipv6 interface [local-chassis <chassis-id> I master] emp
- show ipv6 emp-interfaces

DNS IPv6 Configurable Per Network

The OmniSwitch allows to advertise IPv6 DNS servers in Router Advertisements (RA). This is achieved by including DNS server options within the Router Advertisement messages. The switch uses ra-rdnss-list option that is used to including DNS server options within the Router Advertisement messages, extending ra-send-rdnss per interface.

The following CLI commands are associated with this feature:

- [no] ipv6 ra-rdnss-group <groupname>
- [no] ipv6 ra-rdnss-server <ip6addr> group <groupname>
- ipv6 ra-rdnss-list <groupname> | no ipv6 ra-rdnss-list
- ipv6 interface <ifname>[ra-rdnss-list <groupname> | no ra-rdnss-list]

- [ra-send-rdnss {yes | no}
- show ipv6 router ra-options ra-rdnss-group

The switch uses ra-dnssl-list option that is used to specify a default domain name suffix for DNS searches, extending ra-send-dnssl per interface.

The following CLI commands are associated with this feature:

- [no] ipv6 ra-dnssl-group <groupname>
- [no] ipv6 ra-dnssl-domain <domain> group <groupname>
- ipv6 ra-dnssl-list <groupname> | no ipv6 ra-dnssl-list
- ipv6 interface <ifname>[ra-dnssl-list <groupname> | no ra-dnssl-list]
- [ra-send-dnssl {yes | no}]
- show ipv6 router ra-options ra-dnssl-group

Services Features

EVPN Enhancements

Symmetric based routing (for both host-based and prefix-based routes) will be supported in 8.10.R02. Asymmetric routing for Prefix based routes will not be supported in 8.10.R02.

The operation of the Symmetric L3VPN model is simple in terms of configuration and deployment and also better scalability than the Asymmetric IRB mode, and therefore is the prevalent and recommended configuration for the inter-service routing of EVPN hosts. The symmetric IRB model is used for establishing L3 connectivity for both host-based and prefix-based routes.

In the symmetric IRB solution, a network unique EVI is created on all the PEs for each tenant/VRF of the PE. This EVI is configured as the L3EVI (referred as Fabric-vpn in AOS). Only one Fabric-vpn is required per VRF that will provide the inter-EVI reachability for all the IRB services in the VRF. Additionally, the Fabric-vpn is also used as the gateway for prefix route advertisement for both EVPN and non-EVPN routes.

The following CLI commands are associated with this feature.

- service vpn-type
- show service evpn evi

IP Mobility Service for EVPN

Supports IP mobility or DAD (Duplicate Address Detection). DAD is considered as movement of IP to MAC association. This means two hosts are assigned to the same IP. This could be either because of human error or a spoofing attack on an EVPN network.

The following CLI command is associated with this:

- service bgp-evpn ip-mobility

Service Interface Model

Supports EVPN service interface model on a service. RFC 8388 defines provides three types of EVPN service interface models for provisioning CE-VID to EVI.

AOS will support two models: VLAN-based service interface model and Enhanced VLAN-bundle Service Interface (ALE Defined) model.

In 8.10R02, only Enhanced VLAN-bundle service model is supported. Vlan-based service model is an EA feature.The following CLI command is associated with this:

- service bridge-type

EVPN Service BUM Traffic Management - BUM traffic (Broadcast, Unknown-Unicast and Multicast) traffic can each be managed for the flood or no flood treatment. Any action on each of these traffic type can be configured by enabling or disabling the flood action.

The following CLI command is associated with this:

- service bgp-evpn broadcast

EVPN IP Multicast Support Enhancement

- Multicast is supported in all-active mode for multi-home ethernet segments.
- Static multicast groups are supported on multi-home ethernet segments as well.
- SMET (Selective Multicast) by all PEs

The following CLI commands are associated with this feature:

- service access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [evpn-ethernet-segment {enable | disable}] [multi-homing {all-active | single-active}]
- service service_id igmp-mld-proxy {enable | disable} [smet-on-multihome {df | all}]]

EVPN- BGP Route Reflectors: Intra domain (I-BGP)

To reduce the number of BGP peering within an AS is RR (Route Reflector), rather than each BGP system having to peer with every other BGP system within the AS, each BGP speaker instead peers with a RR. Routing advertisements sent to the RR are then reflected (sent) out to all the other BGP speakers.

AOS supports BGP Route Reflection for EVPN address families. AOS supports Single cluster with one RR and Single cluster with redundant RRs. Number of leafs on each cluster should not exceed 32.

The connection between RR and the leafs on the overlay is iBGP. And the underlay is IGP (OSPF is recommended).

The following CLI commands are associated with this feature:

- No new CLI

MPLS, MPLS VPLS, MPLS VPWS on OS6900

MPLS, MPLS VPLS, and MPLS VPWS are supported on OS6900-X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 models starting in 8.10R2.

MPLS OAM LSP Ping and Traceroute Support

MPLS OAM helps service providers monitor label-switched paths (LSPs) and quickly isolate MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network. One of the important MPLS OAM features is LSP ping and traceroute, which is used to detect and isolate data plane failures in MPLS LSPs when IP reachability and MPLS control plane seem to be working fine.

AOS supports LSP ping and traceroute in accordance with RFC 4379 - Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures.

The following CLI commands are associated with this feature:

- mpls ping ldp
- mpls trace ldp

Virtual Private Wire Service (VPWS) Support

VPWS is a class of VPN service that provides point-to-point (P2P) VPN connectivity service for customers connected to an MPLS network. Based on the MPLS technology, VPWS allows multiple customers to share one transport leased line (LSP) and create an exclusive virtual channel for each customer on the shared LSP. On an Ethernet network, sites in different cities can communicate over a P2P VPWS connection on an MPLS network, just like communicating within a Virtual Local Area Network (VLAN).

The following CLI commands are associated with this feature:

- service vpws
- service description
- service multicast-mode
- service vlan-xlation
- service admin-state
- service remove-ingress-tag
- show service
- show service ports
- show service vpws sap
- show service debug-info
- show service info
- service l2profile
- service access
- service access l2profile
- service access vlan-xlation
- show service l2profile
- show service access
- service sap
- service sap description
- service sap trusted
- service sap stats
- service sap admin-state
- service sdp mpls
- service bind-sdp
- show service sdp
- show service sdp mpls
- show service bind-sdp vpws
- show service vpws mesh-sdp
- show mpls vpws vc-table

Transparent Bridging

VLAN stacking transparent bridging support has been extended to the OS6870.

QoS/Security Features

MACsec Support

Dynamic (128-bit) MACsec is supported on the OS6570M, OS6870, and OS99-CMM2. See Appendix B MACsec table for a list of supported ports and speeds.

The following CLI commands are associated with this feature:

- interfaces macsec admin-state
- interfaces macsec key-rotation max-session-time
- interfaces macsec key-rotation max-exchange-data
- show interfaces macsec

Note: The show interfaces capability command may display 256-bit as supported. This is related to the hardware capability, 256-bit software capability will be supported in an upcoming release.

Option to Disable 'exit-on-fail' for AAA Authentication

A new option (exit-on-fail) is included to enable or disable the switch authentication using all the servers in the list. When the option is enabled the user authentication will take place with the first available server. If the user information is not available in the first available server, the authentication request will fail.

This option is currently applicable only for ASA users accessing the switch through the console, TELNET, FTP, HTTP, SNMP, and SSH sessions. The **exit-on-fail** parameter is enabled by default.

The following CLI commands are associated with this feature:

- aaa authentication {console | telnet | ftp | http | snmp | ssh | default} server1 [server2...] [local] [exit-on-fail {enable | disable}]
- show aaa authentication

Kerberos-snooping on 6870 (VLAN/Service Domain)

Kerberos-snooping support for both the VLAN and service domain is extended to OS6870.

The following CLI commands are associated with this feature:

- unp profile kerberos-authentication
- kerberos inactivity-timer
- kerberos ip-address
- kerberos server-timeout
- kerberos authentication-pass policy-list-name
- kerberos authentication-pass domain
- clear kerberos statistics
- show kerberos configuration
- show kerberos users
- show kerberos statistics

IEEE Drop Enhancement

A new option **ieee-cisco-drop-all** can be configured on a UNI profile to filter IEEE and Cisco protocol packets.

The following CLI commands are associated with this feature:

- ethernet-service uni-profile {ieee-cisco-drop-all | <uprofile-name>} [inbound {tagged | untagged| both}] [L2-protocol {stp | 802.1x | 802.1ab | 802.3ad | gvrp | amap} {peer | discard | mac-tunnel | tunnel}]
- ethernet-service uni {port <slot/port1[-port2]>|linkagg <agg_id>} uni-profile {default-uni-profile | ieee-fwd-all | ieee-drop-all | ieee-cisco-drop-all | <uprofile-name>}
- show ethernet-service uni-profile

Other Features

Precison Time Protocol (PTP) – End-to-End Support

This enhancement adds support for PTP End-to-End on the following platforms and interfaces:

- OS6860N-P48Z –2.5G, 5G, 25G interfaces.
- OS6860N-U28 –25G interfaces.
- OS6900-V48 25G and 100G interfaces.
- OS6870 – All platforms with exceptions below:
    - Except OS6870-24
    - Except OS6870-48

The following CLI commands are associated with this feature:

- interfaces ptp admin-state
- show interfaces ptp config

Storm Control Handling of Unknown Unicast Traffic with Action as Shutdown

This feature is supported on the OS6870 beginning in 8.10R2.

The following CLI commands are associated with this feature:

- interfaces flood-limit uucast action

RAF/ LPND Support

Route Advertisement Filtering (RAF) and Local Proxy Neighbor Discover (LPND) are supported on the OS6870.

The following CLI commands are associated with this feature:

- ipv6 ra-filter
- ipv6 local-proxy-nd

OS6870 TCAM Profiles

The OmniSwitch allows for selecting a different number of TCAM rules for a select application by allowing configuration of different TCAM profiles. The configuration offers default and built-in TCAM profiles. The built-in TCAM profiles are **metro-services, qos-acl, source-ipv6-acl, and bidirectional-ipv6-acl**. The user can configure the required TCAM profile and reload the switch to activate the configured TCAM profile.

The following CLI commands are associated with this feature:

- tcam profile { default | metro-services | qos-acl |bidirectional-ipv6-acl | source-ipv6-acl }
- show tcam profile { default | metro-services | qos-acl |bidirectional-ipv6-acl | source-ipv6-acl }

Feature	Resource Name	Default	Metro services	QoS ACL	Source IPv6 ACL	Bidirectional IPv6 ACL	Description
QoS Policy Rules	QoS Policy Ingress	2048	2048	4096	2048	2048	
QoS Egress Policy Rules	QoS Policy Egress	256	128	128	128	256	
QoS Policy Rules – Bidirectional IPv6	QoS Policy Ingress	N/S	N/S	N/S	N/S	Supported	
SAP Classification Rules	System TTI	2048	4096	1024	1024	2048	Map SVLAN/service to traffic coming on UNI/SAP ports.
VSTK Egress VLAN Translation	VSTK SAP-Profile Egress	256	1024	256	256	256	To replace SVLAN with CVLAN when packet goes out of UNI ports in translate mode.
Service Tunnels	Tunnel Services Ingress	2048	1024	1024	1024	2048	SPB, VxLAN or L2 GRE services creation.
DHCP Snooping ISF IPv4	UDP_RLY_ISF	256	256	256	256	256	
DHCP Snooping ISF IPv6	DHCP6_RLY_ISF	0	0	0	256	0	
UNP Users	AG	2048	1024	1024	1024	2048	
PVLAN Rules	PVLAN Ingress/ Egress	256	256	64	64	256	Ingress rules are for dropping the VLAN traffic and are different from the primary/secondary on the ports.

							Egress rules for translating egress VLAN i.e. If the traffic comes from primary VLAN ports and then egresses out of secondary VLAN tagged ports, the VLAN tag needs to be translated to the secondary VLAN and vice-versa.
QoS Anti Spoofing	QoS-AntiSpoof	256	128	256	128	256	

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release.

System / General / Display		
CR	Description	Workaround
CRAOS8X-23137	When high number of vlans are mapped to DHL links, during failover some traffic loss may be seen.	There is no known workaround at this time.
CRAOS8X-41054	On an OS9912, when upgrading coreboot on both CMMs at the same time and reloading from working, CMM-B becomes primary instead of CMM-A as expected.	Upgrade one CMM at a time.
CRAOS8X-41328	On an OS9912 if a member port of a link aggregate with hashing/load-balancing enabled is disabled all the traffic may be sent on just one of the other ports instead of being load-balanced across the link aggregate.	There is no known workaround at this time.
CRAOS8X-41538	Intermittently (rarely) OS99-CNI-U20 module can fail to come up and park in an unpowered state. A messages similar to the following may be seen on console (and NI swlogs): \+++ NI in slot [s] power-good failure in 3 attempts - disabling	Hot-swap the NI (unplug/replug) or power cycle the chassis.
CRAOS8X-46086	Encountering the error `System is busy. Please try later. (1005)` during bulk VLAN configuration, particularly after executing `no vlan 4092`. This issue is not directly related to the VLAN feature but comes when processing large configuration involving up to 4K static routes across 64 VRFs. The system experiences delays while processing a large number of IP interface commands when applied from configuration file. The error is observed when the system is temporarily in a busy state due to the heavy processing load.	To mitigate the issue, split large configuration files into smaller segments and apply them sequentially. This approach helps avoid timeouts and reduces the system load during configuration processing.
CRAOS8X-47865	Precision Time Protocol (PTP 1588v2) End-to-End Transparent Clock is currently not supported on OS6870-24 and OS6870-48 port models.	There is no known workaround at this time.
CRAOS8X-48631	PTP 1588v2 E2E TC – Issue of high " 2-way time error mean" observed on OS6870-P24Z/P48Z and OS6870-P24M/P48M with expansion modules when PTP packets ingress at copper port and egress out of fiber ports and vice versa.	There is no known workaround at this time.
CRAOS8X-49746	An error occurs when the 50G license is removed from the server by one of the	Use one of the commands below to delete the license:

	commands below or client with the option "50G" option, and the master is not requesting a 50G license. The master will incorrectly determine the license status after removal, and automatically install the demo license. license server remove <node-id/node-ip/site> license 50g license client remove license 50g	license server remove <node-id/node-ip/site> license all license client remove license all
CRAOS8X-48522	On an OS9907 in redundant OS99-CMM2 configuration, the system may experience some instability when performing a management module hot swap.	It is recommended to perform the management module replacement during the scheduled maintenance window. After replacing the module, the operator should verify that the system has stabilized to ensure proper functionality.
Hardware / Transceivers		
CRAOS8X-35816	SFP-10G-T supports only 10G peer links. Link will be down when peer speed is either 1G or 100M. If peer 1G or 100M is left connected, after some idle time, some quick down>up toggles may be seen locally. When peer is changed to 10G, port will operate as expected. However, it has been observed, if peer is left at 100M for a lengthy period, and multiple down>up toggles are seen, port may not recover even after reverting back to 10G.	Recommend peer end to be strictly at 10G.
CRAOS8X-36381	It is possible with SFP-GIG-T , when speed is configured to 10M, multiple admin disable/enable toggles can cause port instability (including false local linkup and no traffic through port). Issue is seen with repeated consecutive local admin disable/enable toggles. Issue is not seen with 1G and 100M speed configurations.	There is no known workaround at this time.
CRAOS8X-36440	U28 port 25 with 10G-T 10G cusfp may see a local only linkup or a LED up with link down when peer side is admin-toggled repeatedly.	
CRAOS8X-36589	SFP-100-BX-U/D may have a linkup without cable on some random ports. Port number and number of ports displaying issue appears to vary by switch (ranging from none up to two ports).	Normal operation is expected when cable is inserted.
CRAOS8X-41609	On 6860N 25G ports with a 4x10G transceiver, on intermittent admin disables one or more ports will continue to display up.	Admin enable the port when peer is disabled or disconnect/remove the transceiver.

CRAOS8X-41611	On an OS99-CNI-U8 with 4x25G DAC link sometimes does not come up for certain lanes.	Use the QSFP-100G-SR4 fiber transceiver with 4X25G capability.
CRAOS8X-43486	On some platforms (OS6860N 25G ports, OS6900 10G and 25G ports, OS6560-P48X4 ports 53/54 and OS6360 uplink ports), the SFP-10G-GIG-LR/SR only links up at 10G and is unstable at 1G speed.	If 1G speed is required, use 1G transceivers.
CRAOS8X-44378	A fake link with SFP-DUAL-BX-D/U on the 25G ports may sometimes be seen.	There is no known workaround at this time.
CRAOS8X-46185	Fiber ports with SFP-GIG-T connected to peer at 10M speed is operational as expected. However, when the peer link changes from 10M to 100M or 1G speed, user may (intermittently) see link down with peer side link up.	On OS6570M-U28 a hot-swap of the SFP-GIG-T recovers the port. On OS6570M-12/12D a switch reload may be required to recover port.
CRAOS8X-46195	VFL links using 4X25G splitters require additional configuration to prevent CRC errors being seen on the link.	The preferred method is configuring inter-frame-gap to 13 on both sides of the link. An alternate method is configuring FEC to FC and auto-negotiation disable on both sides of the link. Note: Configuring FEC and disabling auto-negotiation will cause link to reset.
CRAOS8X-46436	On the uplink ports of some platforms (OS6560-P24X4 & P48X4, OS6560-P24Z24, OS6360-P24X, OS6465-P28), the SFP-10G-GIG-LR/SR only links up at 10G and is unstable at 1G speed.	If 1G speed is required, use 1G transceivers.
CRAOS8X-49127	An issue of slow increment of CRC errors has been observed for random packets with the SFP-GIG-T transceivers on OS6870-P24Z/P48Z 25G ports and OS6870-LNI-U6 50G ports.	There is no known workaround at this time.
Layer 2		
CRAOS8X-26502	While converging due to a link/node failure in a MRP ring network, sometimes a very few multicast IGMP clients are not relearned when there are more than 200 multicast streams.	Clients will be relearned after the next query interval.
CRAOS8X-41707	When configuring erp ring and verify convergence with port down/up and node down/up events, the convergence number is high for an average 10 iterations.	There is no known workaround at this time.
Layer 3		
CRAOS8X-39691	On an OS9912 a BGP neighbor in a VRF may get stuck in idle state after NI reset if the same VLANs are associated to two different NIs.	After approximately 90 seconds the neighbor association will be restored.

CRAOS8X-44230	CRAOS8X-44230 When IPMVLAN is enabled on a switch with rvlan configured on the receiver port, after a write memory flash-synchro and reload, when the ipmvlan configs are removed the slave unit still retains the routing mode on it. Now if IPMVLAN is enabled without rvlan on receiver port and the current slave becomes the master due to VC-takeover, it starts behaving like L3 mode with forward and source table getting populated when source traffic flows.	There is no known workaround at this time.
CRAOS8X-49558	BGP configs are missing after upgrade (standard or ISSU) from 8.10.R1 to 8.10.R2 GA build with MPLS Debian package installed.	After the switch comes up with 8.10.R2 GA build, upgrade to the MPLS Debian package "uos-mpls-v4.deb" version, re-configure all the missing BGP config again and then save the config.
Services		
CRAOS8X-33705	Double tagged packets with size less than 64 bytes received as encapsulated inside a tunneled packet (eg: SPB encapsulated), may get dropped on the network port of an OS6900.	There is no known workaround at this time.
CRAOS8X-49202	EVPN symmetric routing: Routes not getting cleared from FIB with "clear arp-evpn-proxy-cache" . Issue is seen on most of the RIB clearing events like static ARP deletion or proxy aging.	Fabric service toggle is currently not supported.
Virtual Chassis		
CRAOS8X-41294	After 2nd vc-takeover, we could see that sometimes sdp or sap macs are missing from 'show mac-learning' output.	Re-send traffic for missing macs.
CRAOS8X-46025	NTP is not working on port of slave chassis with non-default VRF.	1. Use Port on master for NTP. 2. Or, when using port on slave chassis set the VRF to be used for all NTP operations before enabling NTP service.
CRAOS8X-49745	The 50G license will not be installed on slave units whose demo period has expired. The master unit will remain unaffected.	Install the license before the demo period expires. In a case where the license on the slave units has expired convert the slave unit to a master, install the license on, and then rejoin the virtual chassis.
QoS / Security		
CRAOS8X-34219	With CFM2 and XNI-U48 board, port recovery after violation takes additional 2 mins with WTR of 15 secs.	There is no known workaround at this time.

CRAOS8X-34758	Port violation recovery takes additional 5 secs sometimes.	There is no known workaround at this time.
CRAOS8X-40989	On an OS99-XNI-P24Z8 the dynamic MACsec port status is down after a reload.The issue is only specific to the first 8 ports.	Toggle the MACsec admin state on the port.
CRAOS8X-41038	When configuring static MACsec without encryption and keys are mismatched, the traffic can still go through. Works as expected with encryption enabled.	There is no known workaround at this time.

Hot-Swap/Redundancy Feature Guidelines

Hot-Swap Feature Guidelines

Refer to the table below for hot-swap/insertion compatibility. If the modules or power supplies are not compatible a reboot of the chassis is required after inserting the new component.

- When connecting or disconnecting a power supply to or from a chassis, the power supply must first be disconnected from the power source.
- All NI module extractions must have a 30 second interval before initiating another hot-swap activity. CMM module extractions should have between a 15 and 20 minute interval.
- All new module insertions must have a 5 minute interval AND the LEDs (OK, PRI, VC, NI) have returned to their normal operating state.

Existing Expansion Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS68-XNI-U4	OS68-XNI-U4
OS68-VNI-U4	OS68-VNI-U4
OS68-QNI-U2	OS68-QNI-U2
OS68-CNI-U1	OS68-CNI-U1

OS6860N-P48M Hot-Swap/Insertion Compatibility

Existing Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS99-CMM	OS99-CMM
OS99-CMM2	OS99-CMM2
OS9907-CFM	OS9907-CFM
OS99-GNI-48	OS99-GNI-48
OS99-GNI-P48	OS99-GNI-P48
OS99-XNI-48	OS99-XNI-48
OS99-XNI-U48	OS99-XNI-U48
OS99-XNI-P48Z16	OS99-XNI-P48Z16
OS99-CNI-U8	OS99-CNI-U8
OS99-GNI-U48	OS99-GNI-U48
OS99-XNI-U24	OS99-XNI-U24
OS99-XNI-P24Z8	OS99-XNI-P24Z8
OS99-XNI-U12Q	OS99-XNI-U12Q

OS99-XNI-UP24Q2	OS99-XNI-UP24Q2
OS99-CNI-U20	OS99-CNI-U20

OS9900 Hot-Swap/Insertion Compatibility

Existing Expansion Slot	Hot-Swap/Hot-Insert compatibility
Empty	All modules can be inserted
OS6870-LNI-U6	OS6870-LNI-U6
OS6870-CNI-U2	OS6870-CNI-U2

OS6870 Hot-Swap/Insertion Compatibility

Hot-Swap Procedure

The following steps must be followed when hot-swapping modules.

1. Disconnect all cables from transceivers on module to be hot-swapped.
2. Extract all transceivers from module to be hot-swapped.
3. Extract the module from the chassis and wait approximately 30 seconds before inserting a replacement.
4. Insert replacement module of same type. For a CMM wait approximately 15 to 20 minutes after insertion.
5. Follow any messages that may displayed.
6. Re-insert all transceivers into the new module.
7. Re-connect all cables to transceivers.
8. Hot-swap one CFM at a time. Please ensure all fan trays are always inserted and operational. CFM hot-swap should be completed with 120 seconds.

VC Hot-Swap / Removal Guidelines

Elements of a VC are hot-swappable. They can also be removed from, or added to, a VC without disrupting other elements in the VC. Observe the following important guidelines:

- Hot-swapping an element of a VC is only supported when replaced with the same model element (i.e. an OS6900-V72 must be replaced with an OS6900-V72).
- Replacing an element with a different model element requires a VC reboot.

Fast/Perpetual PoE Unlike Power Supply Swapping

When swapping unlike power supplies on an OS6860N-P48M follow the procedure below to ensure continued PoE functionality when fast or perpetual PoE is enabled.

1. Disable fpoe and ppoe (Only needs to be executed if lanpower is started).
2. Save and synchronize the configuration.
3. Swap the power supplies.
4. Reload chassis.

5. Start lanpower.
6. Enable fpoe and ppoe as required.
7. Save and synchronize the configuration.

Technical Support

ALE technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Country	Supported Language	Toll Free Number
France, Belgium, Luxembourg	French	+800-00200100
Germany, Austria, Switzerland	German	
United Kingdom, Italy, Australia, Denmark, Ireland, Netherlands, South Africa, Norway, Poland, Sweden, Czech Republic, Estonia, Finland, Greece, Slovakia, Portugal	English	
Spain	Spanish	
India	English	+1 800 102 3277
Singapore	English	+65 6812 1700
Hong-Kong	English	+852 2104 8999
South Korea	English	+822 519 9170
Australia	English	+61 2 83 06 51 51
USA	English	+1 800 995 2696
Your questions answered in English, French, German or Spanish.	English French German Spanish	+1 650 385 2193 +1 650 385 2196 +1 650 385 2197 +1 650 385 2198
Fax: +33(0)3 69 20 85 85 **Email**: ale.welcomecenter@al-enterprise.com **Web** : myportal.al-enterprise.com		

Internet: Customers with service agreements may open cases 24 hours a day via the support web page. Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have hardware configuration, module types and version by slot, software version, and configuration file available for each switch.

Severity 1 - Production network is down resulting in critical impact on business—no workaround available.

Severity 2 - Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 - Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 - Information or assistance on product feature, functionality, configuration, or installation.

Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: **/flash/foss**.

The following is in addition to the information found in the **/flash/foss/Legal_Notice.txt** file.

```
FOSS Name : FOSS Version : Name of Applicable License : Pointer to file containing License
Text

libatomic           : 1.0.0      : GPLv3+ & GPLv3+      : /flash/foss/gpl-3.0.txt +
                                   with exceptions &      /flash/foss/gpl-2.0.txt +
                                   GPLv2+ with exceptions /flash/foss/lgpl-2.1.txt +
                                   & LGPLv2+ & BSD        /flash/foss/bsd1.txt
openvswitch         : 2.12.0     : Apache License 2.0   : /flash/foss/Apache-License-2.0.txt
```

Appendix A: Feature Matrix

The following is a feature matrix for AOS Release 8.10R2.

Note: Early availability features are available in AOS and can be configured. However, they have not gone through the complete AOS validation cycle and are therefore not officially supported.

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Management Features											
AOS Micro Services (AMS)	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R1	8.10R2	8.6R1	8.7R1	8.6R1
Automatic Remote Configuration Download (RCL)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
Automatic/Intelligent Fabric	8.7R2	8.5R1	Y	8.9R2	Y	8.7R2	Y	8.10R2	Y	Y	Y
Automatic VC	8.7R2	N	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	N
Bluetooth - USB Adapter with Bluetooth Technology	8.7R2	8.6R2	8.6R2	8.9R2	Y	8.7R1	8.6R2	8.10R2	8.6R2	N	N
Certify On Reboot	N	8.10R2	8.10R2	8.10R2	8.10R2	N	8.10R2	8.10R2	N	N	N
Console Disable	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.10R2	8.6R2	8.7R1	8.6R2
Dying Gasp	8.9R3	Y	Y	8.9R3	Y	8.7R1	Y	8.10R2	N	N	N
Dying Gasp (EFM OAM / Link OAM)	N	8.6R1	8.6R1	8.9R3	8.6R1	8.7R1	8.6R1	8.10R2	N	N	N
EEE support	Y	8.9R1	8.9R1	8.9R2	Y	8.7R1	Y	N	Y	Y	Y
Embedded Python Scripting / Event Manager	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	Y
IP Managed Services	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Hitless Security Patch Upgrade	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1	8.7R1	8.7R1	8.10R2	8.7R1	8.7R1	8.7R1
In-Band Management over SPB	N	N	N	N	8.5R4	8.7R1	8.5R4	8.10R2	8.5R4	8.7R1	8.5R4
ISSU	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
NaaS	8.8R1	8.8R1	8.8R1	8.9R2	8.8R1	8.8R1	8.8R1	8.10R2	8.8R1	8.8R1	8.8R1
NAPALM Support	8.7R2	8.5R1	8.5R1	8.9R2	8.5R1	8.7R1	8.5R1	8.10R2	8.7R2	8.7R2	N
NTP - Version 4.2.8.p11	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.10R2	8.5R4	8.7R1	8.5R4
NTP - IPv6	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	8.7R3	8.7R3	8.10R2	8.7R3	8.7R3	8.7R3
OpenFlow	N	N	N	N	Y	N	N	N	N	N	N
OV Cirrus – Zero touch provisioning	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	N	8.7R2	8.7R2	N
OV Cirrus – Configurable NAS Address	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	N	8.5R4	8.7R1	8.5R4

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/ C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
OV Cirrus – Default Admin Password Change	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	N	8.5R4	8.7R1	8.5R4
OV Cirrus – Managed	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	N	8.5R4	8.7R1	8.5R4
OVSDB	N	N	N	N	N	N	N	N	N	N	N
Package Manager	8.7R2	8.6R2	8.6R2	8.9R2	8.6R2	8.7R1	8.6R2	8.10R2	8.6R2	8.7R1	8.6R2
Readable Event Log	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R1	8.10R2	8.6R1	8.7R1	8.6R1
Remote Chassis Detection (RCD)	N	N	N	N	8.6R2	8.7R1	N	8.10R2	N	8.7R1	Y
SAA	8.7R2	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	8.10R2	8.7R1	8.7R1	Y
SAA SPB	N	N	N	N	Y	8.7R2	Y	8.10R2	8.7R1	8.7R1	8.6R2
SAA UNP	N	Y	N	N	Y	N	Y	N	N	N	N
Signed AOS Image	8.10R1	8.10R1	8.10R1	8.9R4	8.10R1	8.10R1	8.10R1	8.10R2	8.10R1	8.10R1	8.10R1
SNMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Thin Client	8.8R1	8.8R1	8.8R1	8.9R2	8.8R1	8.8R1	8.8R1	N	8.8R1	8.8R1	8.8R1
U-boot Enable/Disable/Authenticate	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	N	8.7R3	N	N	N	8.7R3
UDLD	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	N	X48C4E	EA
USB Disaster Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1 (onie)	Y	8.10R2 (onie)	8.7R1 (onie)	8.7R1 (onie)	Y
USB Flash (AOS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	N	N	N
Virtual Chassis (VC)	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y (9907) N (9912)
Virtual Chassis Split Protection (VCSP)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRF	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRF – IPv6	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRF – DHCP Client	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Web Services & CLI Scripting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Layer 3 Feature Support											
ARP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
BFD	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
BGP/MP-BGP	N	N	N	8.10R2[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
DHCP Client / Server	8.7R2	8.6R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
DHCP Relay	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
DHCPv6 Server	N	N	N	N	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
DHCPv6 Relay	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
DHCP Snooping / IP Source Filtering	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
ECMP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IGMP v1/v2/v3	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
GRE Tunneling	N	N	N	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
IP-IP Tunneling	N	N	N	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv6 - DHCPv6 Snooping	8.7R2	8.6R1	8.6R1	8.9R2	8.5R3	8.7R1	8.5R4	8.10R2	8.6R2	8.7R1	8.7R1
IPv6 - Source filtering	8.7R2	N	8.6R1	8.9R2	8.5R3	8.7R1	8.5R4	8.10R2	8.6R2	8.7R1	8.7R1
IPv6 - DHCP Guard	EA	EA	EA	8.9R2	EA	N	EA	8.10R2	N	N	N
IPv6 - DHCP Client Guard	EA	EA	EA	8.9R2	EA	N	EA	8.10R2	N	N	N
IPv6 - RA Guard (RA filter)	Y	Y	8.5R2	8.9R2	Y	8.7R1	Y	8.10R2	Y	Y	Y
IPv6 - DHCP relay and Neighbor discovery proxy	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
IP Multinetting	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPSec	N	N	N	N	Y	8.7R1	Y	8.10R2	Y	Y	N
ISIS IPv4/IPv6	N	N	N	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
M-ISIS	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	8.5R2
OSPFv2	N	N	8.9R4[1]	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
OSPFv3	N	N	8.9R4[1]	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
RIP v1/v2	N	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
RIPng	N	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/ C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
UDP Relay (IPv4)	8.7R2	8.5R4	8.5R4	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	8.5R4
UDP Relay (IPv6)	8.7R2	8.6R1	8.6R1	8.9R2	8.6R1	8.7R1	8.6R	8.10R2	8.6R1	8.7R1	8.6R1
VRRP v2	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
VRRP v3	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Server Load Balancing (SLB)	N	N	N	N	Y	8.9R4	Y	N	8.9R4	8.9R4	N
Static routing	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Multicast Features											
DVMRP	N	N	N	N	Y	8.7R1	Y	N	8.5R2	8.7R1	N
IP Multicast VLAN (IPMVLAN)	N	8.9R3	8.9R3 Metro	8.9R3	N	N	N	8.10R2	N	N	N
IPv4 Multicast Switching	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Multicast *,G	8.7R2	Y	8.5R2	8.9R2	8.5R2	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv6 Multicast Switching	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-DM	N	N	8.10R1[6]	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-SM	N	N	8.10R1[6]	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-SSM	N	N	8.10R1[6]	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM-SSM Static Map	N	N	N	N	N	N	N	N	N	N	N
PIM-BiDir	N	N	8.10R1[6]	8.9R4[6]	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
PIM Message Packing	N	N	8.10R1[6]	8.9R4[6]	8.6R1	8.7R1	N	8.10R2	8.6R1	8.7R1	N
PIM - Anycast RP	N	N	8.10R1[6]	8.9R4[6]	8.6R2	8.7R1	8.6R2	8.10R2	8.6R2	8.7R1	8.6R2
Monitoring/Troubleshooting Features											
Ping and traceroute	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Policy based mirroring	N	N	N	N	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	8.5R4
Port mirroring	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Port monitoring	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Port mirroring - remote	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	8.6R1
Port mirroring – remote over linkagg	N	N	8.9R3	N	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	8.6R1
RMON	8.7R2	8.5R1	Y	8.9R2	Y	8.8R2	Y	8.10R2	8.8R2	8.8R2	N
SFlow	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Switch logging / Syslog	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
TDR	8.9R3	8.9R3	8.9R3	N	Y	8.9R3	Y	8.10R2	N	N	N
Layer 2 Feature Support											
802.1q	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
DHL	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	N	Y	N
ERP v2	8.9R3	8.5R1	8.5R2	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	8.5R3
HAVLAN	N	EA	N	N	Y	8.8R1	Y	8.10R2	8.6R2	8.7R1	EA
Link Aggregation (static and LACP)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
LLDP (802.1ab)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Loopback detection – Edge (Bridge)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
Loopback detection – SAP (Access)	N	N	N	N	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
MAC Forced Forwarding / Dynamic Proxy ARP	8.7R2	8.7R1	N	8.9R2	8.6R1	N	8.6R1	8.10R2	N	N	N
MPLS – VPLS	N	N	N	N	N	8.9R3	N	N	N	8.10R2	N
MPLS – VPWS	N	N	N	N	N	8.10R2	N	N	N	8.10R2	N
MRP	N	8.7R2	N	N	N	N	8.7R2	N	N	N	N
Port mapping	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	N
Private VLANs (PVLAN)	N	N	N	N	Y	8.7R2	Y	8.10R2	N	8.7R2	N
SIP Snooping	N	N	N	N	Y	N	N	N	N	N	N
Spanning Tree (1X1, RSTP, MSTP)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Spanning Tree (PVST+, Loop Guard)	N	Y	Y	8.9R2	Y	Y	Y	8.10R2	Y	Y	Y
MVRP	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
SPB[2]	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/ C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
SPB - Over Shared Ethernet	N	N	N	N	8.7R1	8.7R1	8.7R1	8.10R2	8.7R1	8.7R1	8.7R1
SPB – HW-based LSP flooding	N	N	N	N	8.6R1	N	8.6R1	8.10R2	N	N	8.5R4
QoS Feature Support											
802.1p / DSCP priority mapping	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv4	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
IPv6	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Auto-Qos prioritization of NMS/IP Phone Traffic	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Auto-Qos – New MAC range	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.10R2	8.5R2	8.7R1	8.5R2
Groups - Port	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - MAC	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Network	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Service	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Map	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups - Switch	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Groups – VLAN	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R1	8.10R2	8.10R1	8.10R1	8.10R1
Ingress/Egress bandwidth limit	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
Per port rate limiting	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	N
Policy Lists	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Policy Lists - Egress	N	N	N	N	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	N
Policy based routing	N	N	N	8.9R4	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	8.9R4
Tri-color marking	N	N	N	N	Y	8.7R1	Y	8.10R2	N	N	N
QSP Profiles 1	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
QSP Profiles 2/3/4	N	N	N	QSP-2 Only	Y	QSP-2 only	Y	QSP-2 only	QSP-2 only	QSP-2 only	N
QSP Profiles 5	8.7R2	8.5R1	Y	Same as QSP-2	8.7R1	Same as QSP-2	8.7R1	Same as QSP-2	Same as QSP-2	Same as QSP-2	Y
RoCEv2	N	N	N	N	N	N	N	N	8.7R2	N	N

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/ C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
Custom QSP Profiles	8.7R2	Y	Y	8.9R2	Y	Y	Y	8.10R2	Y	Y	Y
GOOSE Messaging Prioritization	N	8.7R1	N	N	N	N	8.7R1	N	N	N	N
Metro Ethernet Features											
CPE Test Head	N	8.6R1	8.9R1 Metro	8.9R2	N	N	N	N	N	N	N
Ethernet Loopback Test	N	Y	8.9R1 Metro	8.9R2	8.6R1	N	8.6R1	N	N	N	N
Ethernet Services (VLAN Stacking)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R2	Y	8.10R2	8.5R4	8.7R1	N
Ethernet OAM (ITU Y1731 and 802.1ag)	N	8.5R1	8.9R1 Metro	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	EA
EFM OAM / Link OAM (802.3ah)	N	8.6R1	8.9R1 Metro	8.9R2	8.5R4	8.7R2	8.5R4	8.10R2	N	N	N
Transparent Bridging	N	N	N	N	Y	Y	Y	8.10R2	Y	Y	N
PPPoE Intermediate Agent	N	8.6R1	8.9R1 Metro	8.9R2	N	N	8.6R1	N	N	N	N
Precision Time Protocol (PTP 1588v2) End-to-End Transparent Clock	N	8.5R1	8.7R2	N	Y	8.9R3	Y	8.10R2	N	8.9R3 (except C32E)	N
Precision Time Protocol (PTP 1588v2) Peer-to-Peer Transparent Clock	N	8.8R2	8.7R2	N	N	N	N	N	N	N	N
Precision Time Protocol (PTP 1588v2) Across VC	N	N	N	N	N	N	N	N	N	N	N
Access Guardian / Security Features											
802.1x Authentication	8.7R2	8.5R2	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Access Guardian – Bridge	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R1	8.7R1	Y
Access Guardian - Access	N	N	N	N	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
Application Fingerprinting	N	N	N	N	N	N	N	N	N	N	N
Application Monitoring and Enforcement (Appmon / DPI)	N	N	N	N	Y	8.7R2	N	8.10R2 (EA)	N	N	N
ARP Poisoning Protection	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R2	8.7R1	Y
BYOD - COA Extension support for RADIUS	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
BYOD - mDNS Snooping/Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	N	8.6R2	8.7R1	Y
BYOD - UPNP/DLNA Relay	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	N	8.6R2	8.7R1	Y
BYOD - Switch Port location information pass-through in RADIUS requests	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y
Captive Portal	8.7R2	8.5R4	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R2	8.7R1	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/C32	6900-X48C6/T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
IoT Device Profiling	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	N	8.6R1	8.7R1	8.5R2
IoT Device Profiling (IPv6)	8.7R2	8.7R1	8.7R1	8.9R2	8.7R1[5]	8.9R3	8.7R1[5]	N	8.9R3	8.9R3	8.7R1
Directed Broadcasts – Control	8.7R2	8.5R2	8.5R2	8.9R2	8.5R2	8.7R1	8.5R2	8.10R2	8.7R1	8.7R1	Y
Interface Violation Recovery	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.7R1	8.7R1	Y
Kerberos Snooping	8.7R2	Y	8.6R2	N	8.6R2	Y	8.6R2	8.10R2	8.6R2	Y	8.6R2
L2 GRE Tunnel Access (Edge) (bridge ports)	N	N	Y	N	Y	8.9R1	Y	8.10R2	N	N	Y
L2 GRE Tunnel Access (Edge) (access ports)	N	N	N	N	8.6R1	8.9R1	8.6R1	8.10R2	8.7R1	8.7R2	8.6R1
L2 GRE Tunnel Aggregation	N	N	N	N	Y	8.9R1	Y	8.10R2	8.7R1	8.7R2	Y
Learned Port Security (LPS)	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.5R4	8.7R1	Y
MACsec[3]	N	8.5R1	8.5R4	8.10R2	Y	8.7R1	N	8.10R2	N	X48C4E	8.5R2
MACsec on Network Port for SPB/L2GRE/VxLAN	N	N	N	N	8.9R1 (6860E)	8.9R1	N	8.10R2	N	8.9R1 (X48C4E)	N
Quarantine Manager	N	8.7R2	8.7R2	8.9R2	Y	8.7R2	Y	8.10R2	8.7R2	8.7R2	8.7R2
RADIUS - RFC-2868 Support	8.7R2	8.5R4	8.5R4	8.9R2	8.5R4	8.7R1	8.5R4	8.10R2	8.5R4	8.7R1	8.5R4
Role-based Authentication for Routed Domains	N	N	N	N	8.5R4	8.7R1	8.5R4	8.10R2	8.6R1	8.7R1	8.5R4
Storm Control (flood-limit)	8.7R2	Y	Y	8.9R2	Y	8.7R1	Y	8.10R2	Y	8.7R1	Y
Storm Control (Unknown unicast with action trap/shutdown)	N	N	N	N	Y	N	Y	8.10R2	N	N	N
TACACS+ Client	8.7R2	8.5R1	Y	8.9R2	Y	8.7R1	Y	8.10R2	8.6R1	8.7R1	Y
TACACS+ command based authorization	8.7R2	N	N	8.9R2	Y	8.7R1	Y	8.10R2	8.7R2	8.7R2	N
TACACS+ - IPv6	8.7R3	8.7R3	8.7R3	8.9R2	8.7R3	8.7R3	8.7R3	8.10R2	8.7R3	8.7R3	8.7R3
PoE Features											
802.3af and 802.3at	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
802.3bt	8.7R2	Y	8.6R2	N	N	8.7R1	Y	8.10R2	N	N	N
Auto Negotiation of PoE Class-power upper limit	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
Display of detected power class	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y
LLDP/802.3at power management TLV	8.7R2	8.5R1	Y	N	Y	8.7R1	Y	8.10R2	N	N	Y

Feature	6360	6465	6560	OS6570M	6860(E)	6860N	6865	6870	6900-V72/ C32	6900-X48C6/ T48C6/X48C4E/V48C8/C32E T24C2/X24C2	9900
HPOE support	8.7R2 (95W)	8.5R1 (60W)	Y (95W)	N	Y (60W)	8.7R1 (95W)	Y (75W)	8.10R2	N	N	Y (75W)
Time Of Day Support	8.7R2	8.5R1	Y	N	Y		Y	8.10R2	N	N	Y
Perpetual PoE	8.7R2	N	N	N	Y	Y	Y	8.10R2	N	N	N
Fast PoE	8.7R2	N	N	N	Y	Y	Y	8.10R2	N	N	N
Delayed Start	8.9R3	8.9R3	8.9R3	N	N	N	N	8.10R2	N	N	N
Data Center Features (License May Be Required)											
CEE DCBX Version 1.01	N	N	N	N	N	N	N	N	N	N	N
Data Center Bridging (DCBX/ETS/PFC)	N	N	N	N	N	N	N	N	N	N	N
EVB	N	N	N	N	N	N	N	N	N	N	N
FCoE / FC Gateway	N	N	N	N	N	N	N	N	N	N	N
VxLAN[4]	N	N	N	N	N	8.8R1	N	8.10R2	8.5R3	8.8R1	N
VxLAN EVPN	N	N	N	N	N	N	N	N	N	8.10R1	N
VM/VxLAN Snooping	N	N	N	N	N	N	N	N	N	N	N
FIP Snooping	N	N	N	N	N	N	N	N	N	N	N

Notes:
1. OS6560 supports 2 OSPF areas with Advanced Routing license.
2. See protocol support table in Appendix C.
3. Site license required beginning in 8.6R1.
4. L2 head-end only on OS6900-V72/C32.
5. HTTP IPv6 only supported on OS6860(E) and OS6865
6. Advanced Routing license required.

Appendix B: MACsec Platform Support

The following table lists the platforms and modules that support the MACsec functionality.

MACsec Support (MACsec site license required)	
OmniSwitch 9900	
OS99-CMM	4X10G mode only - Static and Dynamic (128-bit) modes
OS99-CMM2	Ports 1-4 (40G, 100G,4x10G,4x25G) – Dynamic (128-bit) mode
OS99-GNI-48/P48	10M/100M/1G ports - Static and Dynamic (128-bit) modes
OS99-XNI-48/P48	10G ports - Static and Dynamic (128-bit) modes
OS99-XNI-U48	10G ports - Static and Dynamic (128-bit) modes
OS99-XNI-P48Z16	1G/2.5G/5G/10G (16x) - Static and Dynamic (128-bit) modes 1G/10G (32x) - Static and Dynamic (128-bit) modes
OS99-GNI-U48	1G ports - Static and Dynamic (128-bit) modes
OS99-XNI-U24	10G ports - Static and Dynamic (128-bit) modes
OS99-XNI-P24Z8	1G/2.5G/5G/10G (8x) - Static and Dynamic (128-bit) modes 1G/10G (16x) - Static and Dynamic (128-bit) modes
OS99-XNI-U12Q	10G / 4x10G Uplink - Static and Dynamic (128-bit) modes
OS99-XNI-UP24Q2	10G(Fiber)/4x10G Uplink - Static and Dynamic (128-bit) modes 10G (Copper) - Static and Dynamic (128-bit) modes
OS99-CNI-U8	Not Supported
OS99-CNI-U20	40G/100G - Static and Dynamic (128-bit) modes
OmniSwitch 6900	
OS6900-X48C4E	Dynamic mode only on all ports. Supports 256-bit key length.
OmniSwitch 6870	Dynamic (128-bit) mode
OS6870-24	Port 1-24 (10M,100M,1G) Port 25-26 - Not Supported Port 27-30 (10G, 25G)
OS6870-P24M	Port 1-24 (1G, 2.5G, 5G, 10G) Port: 25-26 (40G, 100G, 200G, 4X10G, 4X25G)
OS6870-P24Z	Port 1-24 (100M,1G,2.5G) Port: 25-26 (40G, 100G,4x10G,4x25G) Port 27-32 (10G, 25G)
OS6870-48	Port 1-48 (10M,100M,1G) Port 49-50 - Not Supported Port 51-54 (10G, 25G)
OS6870-P48M	Port 1-48 (1G, 2.5G, 5G, 10G) Port: 49-50 (40G, 100G, 200G, 4X10G, 4X25G)
OS6870-P48Z	Port 1-48 (100M,1G,2.5G) Port: 49-50 (40G, 100G, 4x10G, 4x25G) Port 51-56 (10G, 25G)
OS6870-V12	Port 1-12 (10G, 25G) Port: 13-14 (40G, 100G, 200G, 4X10G, 4X25G)
OS6870-CNIU2	Port 1-2 (40G, 100G, 4x10G, 4x25G)
OS6870-LNIU6	Port 1-6 (10G,25G,50G)
OmniSwitch 6860(E)	
OS6860(E)	All models support MACsec on 10G ports.
OS6860E-P24	1G/10G ports.
OS6860E-P24Z8	1G/10G ports (not supported on 2.5G ports).
OmniSwitch 6860N	Dynamic mode only. All OS6860N models support 256-bit key length.

OS6860N-U28	SFP (1-24), SFP+ (25-28) and SFP28 (31-34) ports
OS6860N-P48Z	SFP28 (51-54) ports
OS6860N-P48M	- Expansion modules (Not supported on any 4X10G splitter transceivers). - Multi-rate Gigabit Ports (37-48)
OS6860N-P24Z	SFP28 (27-30) ports
OS6860N-P24M	- Expansion modules (Not supported on any 4X10G splitter transceivers) - Multi-rate Gigabit Ports (1-24)
OmniSwitch 6570M	Dynamic (128-bit) mode
OS6560M-12/12D	Ports 1-8 (10M/100M/1G) Ports 9-10 (1G) Ports 11-12 (1G/10G)
OS6570M-U28	Ports 1-24 (1G) Ports 25-30 (1G/10G)
OmniSwitch 6560(E)	
OS6560-P24X4/24X4	- Ports 1-24 (Static and Dynamic modes) - Ports 25-30 (Not Supported)
OS6560-P48X4/48X4	- Ports 1-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-P48Z16 (904044-90 only)	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560E-P48Z16	- Ports 1-32 (Static and Dynamic Modes) - Ports 33-48 (Static and Dynamic modes) - Ports 49-52 (Dynamic mode only) - Ports 53-54 (Not Supported)
OS6560-X10	- Ports 1-8 (10G ports only. Dynamic mode only) - Ports 9-10 (Not Supported)
OmniSwitch 6465	- OS6465-P28 - Supported on all ports except ports 27 and 28. - OS6465T-12 and OS6465T-P12 – Not supported on ports 11 and 12. - All other models support MACsec on all ports.

Appendix C: SPB L3 VPN-Lite Service-based (Inline Routing) / External Loopback Support / BVLAN Guidelines

The OmniSwitch supports SPB L3 VPN-Lite using either service-based (inline routing) or external loopback. The tables below summarize the currently supported protocols for each method in this release.

OmniSwitch Inline Routing Support								
	9900	6900-V72/C32 (Front panel port)	6900-T48C6/X48C6	6900-X48C4E/V48C8	6900-C32E	6860N	6900-X/T24C2	6870
IPv4 Protocols								
Static Routing	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
RIP v1/v2	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
OSPF	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
BGP	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
VRRP	Y	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IS-IS	N	N	N	N	N	N	N	N
PIM-SM/DM	8.5R3	8.6R2	Y	Y	8.8R1	Y	8.9R1	8.10R2
DHCP Relay	8.5R3	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
UDP Relay	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
DVMRP	N	N	N	N	N	N	N	N
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IGMP Snooping	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IP Multicast Headend Mode	Y	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IP Multicast Tandem Mode	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1	8.10R2
IPv6 Protocols								
Static Routing	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
RIPng	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
OSPFv3	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
BGP	8.5R4	8.6R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
VRRPv3	8.5R4	8.7R1	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IS-IS	N	N	N	N	N	N	N	N
PIM-SM/DM	8.5R4	8.6R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1	8.10R2
DHCP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
UDP Relay	8.6R1	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
BFD	8.7R2	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IPv6 MLD Snooping	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IPv6 Multicast Headend Mode	Y	8.7R2	8.7R2	8.7R3	8.8R1	8.7R2	8.9R1	8.10R2
IPv6 Multicast Tandem Mode	8.5R4	8.7R2	8.8R1	8.8R1	8.8R1	8.8R1	8.9R1	8.10R2

External Loopback Support								
	OmniSwitch 9900	OmniSwitch 6860/6865	OmniSwitch 6860N	OmniSwitch 6900-V72/ C32	OmniSwitch 6900-X48C6/ T48C6	OmniSwitch 6900-X48C4E	OmniSwitch 6900-V48C8	OmniSwitch 6900-X/T48C2
IPv4 Protocols								
Static Routing	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIP v1/v2	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPF	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRP	8.6R1	8.5R4	8.7R1	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DVMRP	N	N	N	N	N	N	N	N
BFD	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IGMP Snooping	8.5R4	Y	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Headend Mode	8.5R4	Y	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
IP Multicast Tandem Mode	8.5R4	Y	8.7R1	8.6R1	Y	Y	Y	8.9R1
IPv6 Protocols								
Static Routing	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
RIPng	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
OSPFv3	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
BGP	8.5R4	Y	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
VRRPv3	8.5R4	8.5R4	8.7R1	8.7R1	8.7R2	8.7R2	8.7R3	8.9R1
IS-IS	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
PIM-SM/DM	8.5R4	8.5R4	8.7R1	8.5R4	8.7R1	8.7R2	8.7R3	8.9R1
DHCP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
UDP Relay	8.6R1	8.6R1	8.7R1	8.6R1	8.7R1	8.7R2	8.7R3	8.9R1
BFD	Y	Y	Y	Y	Y	8.7R2	8.7R3	8.9R1
IPv6 MLD Snooping	8.5R4	Y	8.7R1	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Headend Mode	8.5R4	Y	8.7R1	Y	8.7R2	8.7R2	8.7R3	8.9R1
IPv6 Multicast Tandem Mode	8.5R4	Y	8.7R1	Y	Y	Y	Y	8.9R1

SPB BVLAN Scalability and Convergence Guidelines

If services are distributed across more than 4 BVLANs in the network it is recommended to consolidate them among just 4 BVLANs. This will reduce the scale of address updates that will happen in the control plane and also help improve network scalability, stability and convergence. Modifying the service BVLAN association is currently not supported. The service will need to be deleted and recreated on the new BVLAN, therefore it's suggested that the consolidation be done during a maintenance window to prevent network disruption.

In most SPB networks this is not a local operation on a single switch. The BVLAN is configured on all the switches in the network. A check must be performed to see if any service has been attached to the BVLAN. The check does not have to be on a local switch, the service attachment to the BVLAN can be on any switch in the network.

1. This will indicate that this is an active BVLAN.
2. Even if the service is not local to a node the node can act as a transit node for the active BVLAN. For this reason the BVLAN cannot be deleted from the network.

To determine if a BVLAN is active use the following command. If there is a service associated with the BVLAN then **In Use** will show as **Yes**. This is a network wide view so even if the services are active on a remote node, this local node will show that the BLVAN is active even if the services are not configured on the local node.

```
OS6860-> show spb isis bvlans
SPB ISIS BVLANS:
                                                                    Services  Num    Tandem
Root Bridge
BVLAN   ECT-algorithm     In Use  mapped    ISIDS  Multicast  (Name : MAC Address)
-------+-----------------+-------+---------+------+----------+-------------------------------
---------
  4000  00-80-c2-01       YES     YES           5  SGMODE
  4001  00-80-c2-02       NO      NO            0  SGMODE
```

After the services have been consolidated the idle BVLANs can be deleted across the entire network. Deleting idle BVLANs will have no effect on the existing network.

Appendix D: General Upgrade Requirements and Best Practices

This section is to assist with upgrading an OmniSwitch. The goal is to provide a clear understanding of the steps required and to answer any questions about the upgrade process prior to upgrading. Depending upon the AOS version, model, and configuration of the OmniSwitch various upgrade procedures are supported.

Standard Upgrade - The standard upgrade of a standalone chassis or virtual chassis (VC) is nearly identical. All that's required is to upload the new image files to the *Running* directory and reload the switch. In the case of a VC, prior to rebooting the Master will copy the new image files to the Slave(s) and once the VC is back up the entire VC will be synchronized and running with the upgraded code.

ISSU - The In Service Software Upgrade (ISSU) is used to upgrade the software on a VC or modular chassis with minimal network disruption. Each element of the VC is upgraded individually allowing hosts and switches which are dual-homed to the VC to maintain connectivity to the network. The actual downtime experienced by a host on the network should be minimal but can vary depending upon the overall network design and VC configuration. Having a redundant configuration is suggested and will help to minimize recovery times resulting in sub-second convergence times.

Virtual Chassis - The VC will first verify that it is in a state that will allow a successful ISSU upgrade. It will then copy the image and configuration files of the ISSU specified directory to all of the Slave chassis and reload each Slave chassis from the ISSU directory in order from lowest to highest chassis-id. For example, assuming chassid-id 1 is the Master, the Slave with chassis-id 2 will reload with the new image files. When Slave chassis-id 2 has rebooted and rejoined the VC, the Slave with chassis -id 3 will reboot and rejoin the VC. Once the Slaves are complete they are now using the new image files. The Master chassis is now rebooted which causes the Slave chassis to become the new Master chassis. When the original Master chassis reloads it comes back as a Slave chassis. To restore the role of Master to the original Master chassis the current Master can be rebooted and the original Master will takeover, re-assuming the Master role.

Modular Chassis - The chassis will first verify that it is in a state that will allow a successful ISSU upgrade. It will then copy the image and configuration files of the ISSU specified directory to the secondary CMM and reload the secondary CMM which becomes the new primary CMM. The old primary CMM becomes the secondary CMM and reloads using the upgraded code. As a result of this process both CMMs are now running with the upgraded code and the primary and secondary CMMs will have changed roles (i.e., primary will act as secondary and the secondary as primary). The individual NIs can be reset either manually or automatically (based on the NI reset timer).

Supported Upgrade Paths and Procedures

The following releases support upgrading using ISSU. All other releases support a Standard upgrade only.

Platform	AOS Releases Supporting ISSU to 8.10R2 (GA)
OS6360	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6465	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6560	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6560E	8.10.115.R01 (MR) 8.10.102.R01 (GA)
OS6570M	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6860(E)	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.92.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6860N	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.92.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6865	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.92.R04 (GA) 8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6900-V72/C32/C32E X48C6/T48C6/V48C8/ X24C2/T24C2	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.92.R04 (GA)

	8.9.221.R03 (GA) 8.9.107.R02 (GA)
OS6900-X48C4E	8.10.115.R01 (MR) 8.10.102.R01 (GA) 8.9.94.R04 (GA)
OS9900 (OS9907)	8.10.102.R01 (GA) 8.9.94.R04 (GA) 8.9.221.R03 (GA)
• ISSU from 8.9.92.R04 is not supported on platforms: OS6360, OS6465, OS6560, OS6570M, OS9900 (due to SSH issue on build 8.9.92.R04) • OS6900-X48C4E VC support introduced in 8.9.R04.	

8.10R2 ISSU Supported Releases

Prerequisites

These upgrade instructions require that the following conditions exist, or are performed, before upgrading. The person performing the upgrade must:

- Be the responsible party for maintaining the switch's configuration.
- Be aware of any issues that may arise from a network outage caused by improperly loading this code.
- Understand that the switch must be rebooted and network access may be affected by following this procedure.
- Have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port.
- Read the GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of U-Boot and FPGA. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.
- Depending on whether a standalone chassis or VC is being upgraded, upgrading can take from 5 to 20 minutes. Additional time will be needed for the network to re-converge.

- The examples below use various models and directories to demonstrate the upgrade procedure. However, any user-defined directory can be used for the upgrade.
- If possible, have EMP or serial console access to all chassis during the upgrade. This will allow you to access and monitor the VC during the ISSU process and before the virtual chassis has been re-established.
    - Knowledge of various aspects of AOS directory structure, operation and CLI commands can be found in the Alcatel-Lucent OmniSwitch User Guides. Recommended reading includes:
        - Release Notes - for the version of software you're planning to upgrade to.
        - The AOS Switch Management Guide
            - Chapter – Getting Started
            - Chapter - Logging Into the Switch
            - Chapter - Managing System Files

- Chapter - Managing CMM Directory Content
- Chapter - Using the CLI
- Chapter - Working With Configuration Files
- Chapter - Configuring Virtual Chassis

Do not proceed until all the above prerequisites have been met. Any deviation from these upgrade procedures could result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

Switch Maintenance

It's recommended to perform switch maintenance prior to performing any upgrade. This can help with preparing for the upgrade and removing unnecessary files. The following steps can be performed at any time prior to a software upgrade. These procedures can be done using Telnet and FTP, however using SSH and SFTP/SCP are recommended as a security best-practice since Telnet and FTP are not secure.

1. Use the command '**show system**' to verify current date, time, AOS and model of the switch.

```
OS6860-> show system
System:
 Description:  Alcatel-Lucent OS6860-P24 8.9.94.R04 GA, March 28, 2024.,
 Object ID:    1.3.6.1.4.1.6486.801.1.1.2.11.1.2,
 Up Time:      88 days 2 hours 1 minutes and 44 seconds,
 Contact:      Alcatel-Lucent, https://www.al-enterprise.com,
 Name:         OS6860,
 Location:     Unknown,
 Services:     78,
 Date & Time:  FRI OCT 11 2024 06:55:43 (PDT)
Flash Space:
 Primary CMM:
  Available (bytes):  1084694528,
    Comments         :  None
```

2. Remove any old tech_support.log files, tech_support_eng.tar files:

```
OS6860-> rm *.log
OS6860-> rm *.tar
```

3. Verify that the **/flash/pmd** and **/flash/pmd/work** directories are empty. If they have files in them check the date on the files. If they are recently created files (<10 days), contact Service & Support. If not, they can be deleted.

4. Use the '**show running-directory**' command to determine what directory the switch is running from and that the configuration is certified and synchronized:

```
OS6860-> show running-directory
CONFIGURATION STATUS
Running CMM              : MASTER-PRIMARY,
CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot         : CHASSIS-1 A,
Running configuration    : vc_dir,
Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
Running Configuration    : SYNCHRONIZED
```

If the configuration is not certified and synchronized, issue the command '**write memory flash-synchro**':

```
OS6860-> write memory flash-synchro
```

6. If you do not already have established baselines to determine the health of the switch you are upgrading, now would be a good time to collect them. Using the show tech-support series of commands is an excellent way to collect data on the state of the switch. The show tech support commands automatically create log files of useful show commands in the **/flash** directory. You can create the tech-support log files with the following commands:

```
OS6860-> show tech-support
OS6860-> show tech-support layer2
OS6860-> show tech-support layer3
```

Additionally, the **'show tech-support eng complete'** command will create a TAR file with multiple tech-support log files as well as the SWLOG files from the switches.

```
OS6860-> show tech-support eng complete
```

It is a good idea to offload these files and review them to determine what additional data you might want to collect to establish meaningful baselines for a successful upgrade.

- If upgrading a standalone chassis or VC using a standard upgrade procedure please refer to Appendix E for specific steps to follow.
- If upgrading a VC using ISSU please refer to Appendix F for specific steps to follow.

Appendix E: Standard Upgrade - OmniSwitch Standalone or Virtual Chassis

These instructions document how to upgrade a standalone or virtual chassis using the standard upgrade procedure. Upgrading using the standard upgrade procedure consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go to the Service and Support website and download and unzip the upgrade files for the appropriate model and release. The archives contain the following:

- OS6360 – Nosa.img
    - Refer to Appendix G for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 – Nos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 – Nos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 – Uos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N – Uosn.img
    - Refer to Appendix H for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS6865 – Uos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 – Yos.img.
    - Refer to Appendix H for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS9900 – Mos.img, Mhost.img, Meni.img
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

2. FTP the Upgrade Files to the Switch

FTP the image files to the *Running* directory of the switch you are upgrading. The image files and directory will differ depending on your switch and configuration.

3. Upgrade the image file

Follow the steps below to upgrade the image files by reloading the switch from the *Running* directory.

```
OS6860-> reload from working no rollback-timeout
```

```
Confirm Activate (Y/N) : y
This operation will verify and copy images before reloading.
It may take several minutes to complete....
```

If upgrading a VC the new image file will be copied to all the Slave chassis and the entire VC will reboot. After approximately 5-20 minutes the VC will become operational.

4. Verify the Software Upgrade

Log in to the switch to confirm it is running on the new software. This can be determined from the login banner or the **show microcode** command.

```
OS6860-> show microcode
/flash/working
Package           Release                 Size     Description
------------------+-----------------------+--------+-----------------------------------
Uos.img           8.10.105.R02             239607692 Alcatel-Lucent OS


OS6860-> show running-directory
CONFIGURATION STATUS
Running CMM              : MASTER-PRIMARY,
CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot         : CHASSIS-1 A,
Running configuration    : WORKING,
Certify/Restore Status   : CERTIFY NEEDED
SYNCHRONIZATION STATUS
Running Configuration    : SYNCHRONIZED
```

Note: If there are any issues after upgrading the switch can be rolled back to the previous certified version by issuing the **reload from certified no rollback-timeout** command.

5. Certify the Software Upgrade

After verifying the software and that the network is stable, use the following commands to certify the new software by copying the *Running* directory to the Certified directory.

```
OS6860-> copy running certified

-> show running-directory
CONFIGURATION STATUS
Running CMM              : MASTER-PRIMARY,
CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot         : CHASSIS-1 A,
Running configuration    : WORKING,
Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
Running Configuration    : SYNCHRONIZED
```

Appendix F: ISSU – OmniSwitch Chassis or Virtual Chassis

These instructions document how to upgrade a virtual chassis using ISSU. Upgrading using ISSU consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go to the Service and Support Website and download and unzip the ISSU upgrade files for the appropriate platform and release. The archive contains the following:

- OS6360 – Nosa.img
    - Refer to Appendix G for recommended/required FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6465 – Nos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6560 – Nos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6570M – Wos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860 – Uos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6860N – Uosn.img
    - Refer to Appendix H for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS6865 – Uos.img
    - Refer to Appendix G for recommended FPGA/U-boot upgrades. AOS must be upgraded prior to upgrading the FPGA/U-boot.
- OS6900 – Yos.img.
    - Refer to Appendix H for recommended CPLD upgrades. AOS must be upgraded prior to upgrading the CPLD.
- OS9900 – Mos.img, Mhost.img, Meni.img
- ISSU Version File – issu_version
- imgsha256sum (not required) –This file is only required when running in Common Criteria mode. Please refer to the Common Criteria Operational Guidance Document for additional information.

Note: The following examples use **issu_dir** as an example ISSU directory name. However, any directory name may be used. Additionally, if an ISSU upgrade was previously performed using a directory named **issu_dir**, it may now be the *Running Configuration*, in which case a different ISSU directory name should be used.

2. Create the new directory on the Master for the ISSU upgrade:

```
OS6860-> mkdir /flash/issu_dir
```

3. Clean up existing ISSU directories
(**Note**: If upgrading a standalone (VC-of-1), modular OS9900 with dual CMMs, skip to step 7).

It is important to connect to the Slave chassis and verify that there is no existing directory with the path **/flash/issu_dir** on the Slave chassis. ISSU relies upon the switch to handle all of the file copying and directory creation on the Slave chassis. For this reason, having a pre-existing directory with the same name on the Slave chassis can have an adverse effect on the process. To verify that the Slave chassis does not have an existing directory of the same name as the ISSU directory on your Master chassis, use the internal VF-link IP address to connect to the Slave. In a multi-chassis VC, the internal IP addresses on the Virtual Fabric Link (VFL) always use the same IP addresses: 127.10.1.65 for Chassis 1,127.10.2.65 for Chassis 2, etc. These addresses can be found by issuing the debug command '**debug show virtual-chassis connection**' as shown below:

```
OS6860-> debug show virtual-chassis connection
                                Address             Address
Chas  MAC-Address          Local IP             Remote IP          Status
-----+------------------+--------------------+------------------+-------------
1       e8:e7:32:b9:19:0b  127.10.2.65       127.10.1.65       Connected
```

4. SSH to the Slave chassis via the internal virtual-chassis IP address using the password 'switch':

```
OS6860-> ssh 127.10.2.65
Password:switch
```

5. Use the **ls** command to look for the directory name being used for the ISSU upgrade. In this example, we're using **/flash/issu_dir** so if that directory exists on the Slave chassis it should be deleted as shown below. Repeat this step for all Slave chassis:

```
OS6860-> rm -r /flash/issu_dir
```

6. Log out of the Slave chassis:

```
OS6860-> exit
logout
Connection to 127.10.2.65 closed.
```

7. On the Master chassis copy the current *Running* configuration files to the ISSU directory:

```
OS6860-> cp /flash/working/*.cfg /flash/issu_dir
```

8. FTP the new image files to the ISSU directory. Once complete verify that the ISSU directory contains only the required files for the upgrade:

```
OS6860-> ls /flash/issu_dir
Uos.img       issu_version  vcboot.cfg    vcsetup.cfg
```

9. Upgrade the image files using ISSU:

```
OS6860-> issu from issu_dir
Are you sure you want an In Service System Upgrade? (Y/N) : y
```

During ISSU '**show issu status**' gives the respective status (pending, complete, etc)

```
OS6860-> show issu status
Issu pending
```

This indicates that the ISSU is completed

```
OS6860-> show issu status
Issu not active
```

Allow the upgrade to complete. DO NOT modify the configuration files during the software upgrade. It normally takes between 5 and 20 minutes to complete the ISSU upgrade. Wait for the System ready or [L8] state which gets displayed in the ssh/telnet/console session before performing any write-memory or configuration changes.

```
OS6860-> debug show virtual-chassis topology
Local Chassis: 1
Oper                                      Config   Oper                      System
Chas  Role         Status              Chas ID  Pri   Group  MAC-Address        Ready
-----+------------+-------------------+--------+-----+------+------------------+-------
1     Master        Running             1        100   19     e8:e7:32:b9:19:0b  Yes
2     Slave         Running             2        99    19     e8:e7:32:b9:19:43  Yes
```

10. Verify the Software Upgrade

Log in to the switch to confirm it is running on the new software. This can be determined from the login banner or the **show microcode** command**.**

```
OS6860-> show microcode
/flash/working
Package           Release                  Size      Description
-----------------+------------------------+--------+---------------------------
Uos.img           8.10.105.R02              239607692 Alcatel-Lucent OS
```

11. Certify the Software Upgrade

After verifying the software and that the network is stable, use the following commands to certify the new software by copying the *Running* directory to the Certified directory:

```
OS6860-> write memory flash-synchro

OS6860-> show running-directory
CONFIGURATION STATUS
Running CMM              : MASTER-PRIMARY,
CMM Mode                 : VIRTUAL-CHASSIS MONO CMM,
Current CMM Slot         : CHASSIS-1 A,
Running configuration    : issu_dir,
Certify/Restore Status   : CERTIFIED
SYNCHRONIZATION STATUS
Flash Between CMMs       : SYNCHRONIZED
Running Configuration    : SYNCHRONIZED
```

Appendix G: FPGA / U-boot Upgrade Procedure

The following CRs or features can be addressed by performing an FPGA/CPLD or U-boot upgrade on the respective models.

CR / Feature	Summary	
CRAOS8X-12042	Description	Switch does not shutdown after crossing danger threshold temperature.
	FPGA Version	0.7
	Platforms	OS6465-P28
CRAOS8X-7207	Description	Chassis reboots twice to join a VC.
	FPGA Version	0.7
	Platforms	OS6560-P24Z24,P24Z8,P48Z16 (903954-90)
CRAOS8X-4150	Description	VC LED status behavior.
	U-boot Version	0.12
	Platforms	OS6865-U28X
8.7R1 Release		
CRAOS8X-16452	Description	Port remains UP when only SFP is connected.
	FPGA Version	- 0.6 (OS6560-P48Z16 (904044-90)) - 0.7 (OS6560-48X4, OS6560-P48X4) - 0.8 (OS6560-X10)
	Platforms	OS6560-P48Z16 (904044-90), OS6560-48X4, OS6560-P48X4, OS6560-X10
Fast/Perpetual PoE	Description	Fast and Perpetual PoE Support
	FPGA Version	0.7 (OS6860E-P24Z8) 0.10 0.14 (OS6865-U28X) 0.25 (OS6865-P16X/U12X)
	Platforms	OS6860/OS6865
8.7R2 Release		
CRAOS8X-4813/13440	Description	U-boot unable to mount NAND flash with UBIFS errors
	U-boot Version	8.7.2.R02
	Platforms	OS6465(T), 6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-13819	Description	U-boot unable to mount eUSB flash
	U-boot Version	8.7.2.R02
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (all PNs), 6865
CRAOS8X-22857	Description	OS6560-P24Z24 reloads continuously with pmds
	FPGA Version	0.8
	Platforms	OS6560-24Z24/P24Z24/24Z8/P24Z8/P48Z16 (903954-90)
1588v2 Support	Description	1588v2 Support
	FPGA Version	0.7 (OS6560-P48Z16 (904044-90)) 0.8 (OS6560-48X4/P48X4)
	Platforms	OS6560-48X4/P48X4/P48Z16(904044-90) Supported on 1G and 10G ports only. Not supported 2.5G ports.
U-boot Password Authentication	Description	U-boot password support (Early Availability)
	U-boot Version	8.7.2.R02
	Platforms	OS6465

8.7R3 Release		
CRAOS8X-26370 CRAOS8X-25033	Description	Required upgrade to enable 12V Power Fail Interrupt (CRAOS8X-26370). Required upgrade to address fan speed issue. (CRAOS8X-25033)
	FPGA Version	0.17
	Platforms	OS6360-24/P24/48/P48
CRAOS8X-24464	Description	U-boot update for CRAOS8X-24464, ability to disable / authenticate U-boot access.
	U-boot Version	8.7.30.R03
	Platforms	OS6360, 6465, 6560, 6860, 6865, 9900. (Not applicable for platforms that use ONIE)
8.8R1 Release		
Boot from USB	Description	U-boot update to allow switch to boot from USB.
	U-boot Version	8.8.33.R01
	Platforms	OS6465, OS6865
8.8R2 Release		
Future compatibility	Description	U-boot/FPGA update to allow future CMM2/OS9912 NI compatibility.
	U-boot/FPGA Versions	See OS9900 Table for versions.
	Platforms	9907
8.9R1 Release		
N/A	There are no U-boot/FPGA upgrade requirements in this release.	
8.9R2 Release		
Fan Speed	Description	Reduced fan speed at boot-up
	FPGA Version	0.20
	Platforms	OS6360-(P)24/(P)48/PH48
CRAOS8X_35470 and CPLD Support	Description	U-boot fix for NAND flash bad file system block. Support of Gowin CPLD[1]
	U-boot	8.9.85.R02
	Platforms	OS6360 (All)
CPLD Support	Description	Support of Gowin CPLD[1]
	U-boot	8.9.92.R02
	Platforms	OS6570M-12/12D/U28
CRAOS8X_35470	Description	U-boot fix for NAND flash bad file system block
	U-boot/FPGA Versions	8.9.85.R02
	Platforms	OS6465 (All), OS6560-(P)24X4/(P)48X4/X10
1. Existing switches do not contain the new CPLD component and do not need to upgrade. Switches with the new CPLD component will ship from the factory with the correct version.		
8.9R3 Release		
CRAOS8X-40924	Description	Address issue when disabling U-boot access.
	U-boot Version	8.9.139.R03
	Platforms	OS6570M-12/12D/U28
Power Supply Interrupt	Description	Address power supply interrupt issue.
	FPGA Version	0.12
	Platforms	OS6570M-U28

8.9R4 Release		
Signed AOS Images	Description	Adds support for signed images when used with AOS 8.9R4 GA release.
	U-boot Version	8.9.70.R04
	Platforms	OS6570M-12/12D/U28
8.10R1 Release		
CRAOS8X-43592	Description	1G/10G SFP not recognized.
	U-boot Version	XNI_U24 - 2.12.0 XNI_U48 - 2.12.0 GNI_U48 - 1.8.0 CNI_U8 - 1.10
	Platforms	OS9907/OS9912
8.10R2 Release		
CRAOS8X-44063	Description	Switches stuck in Marvel mode during bootup.
	U-boot Version	8.10.42.R02
	Platforms	6360, 6465, OS6560-24X4/P24X4/48X4/P48X4/X10
CRAOS8X-44607	Description	Switch stuck in Marvel mode after power cycle.
	U-boot Version	8.10.42.R02
	Platforms	6360, 6465, 6560, 6570M, 6860(E), 6865
CRAOS8X-46275	Description	Switch stuck in Marvel mode after power cycle.
	U-boot Version	8.10.42.R02
	Platforms	6360, 6465, OS6560-24Z8/P24Z8(E)/24Z24/P24Z24/P48Z16(E), 6570M, 6860(E), 6865
Note: The CRs above were also fixed with U-boot version 8.10.115.R01 in the 8.10R1 maintenance release. Switches running 8.10.115.R01 do not need to upgrade to 8.10.42.R02.		

Note: AOS must be upgraded prior to performing an FPGA/CPLD or U-boot upgrade.

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain an FPGA upgrade kit and U-boot file, for example.

- CPLD File - fpga_kit_9022
- u-boot.8.10.R02.42.tar.gz

2. FTP (Binary) the files to the **/flash** directory on the primary CMM.

3. Enter the following to upgrade the FPGA. The **'all'** parameter should be used when upgrading with an FPGA kit. Additionally, this will update all the elements of a VC, for example:

```
-> update fpga-cpld cmm all file fpga_kit_9022
Parse /flash/fpga_kit_9022
fpga file: OS6360-10_CPLD_V19_20230110.vme
Please wait...
fpga file: OS6360-10_CPLD_V19_20230110.vme
update chassis 1
Starting CMM ALL FPGA Upgrade
CMM 1/1
Successfully updated
Reload required to activate new firmware.
```

4. If required, a u-boot upgrade can then be performed, for example:

```
-> update uboot cmm all file /flash/u-boot.8.10.R02.42.tar.gz
Starting CMM ALL UBOOT Upgrade
Please wait...
CMM 1/1
u-boot-ppc_2040.bin: OK
U-boot successfully updated
Successfully updated
```

5. Once complete, a reboot is required.

Appendix H: CPLD Upgrade Procedure for ONIE-Based Devices

The following CRs or features can be addressed by performing a CPLD upgrade on the respective models. Follow the guidelines in the General Upgrade Requirements and Best Practices appendix prior to upgrading.

8.8R2 Release		
OS6860N-P48M/P48Z/P24M/P24Z		
CRAOS8X-29731/30471	Description	OS6860N power supplies
	CPLD File	os6860n_p48m_p48z_u28_maincpu_20220318.updater os6860n_p24m_p24z_maincpld_22020309.updater
8.9R1 Release		
OS6900-T48C6		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
No CR	Description	Improved power down sequence when PSU shut down.
	CPLD File	os6900_t48c6_mainpld_v1.03.02.04.jbc.updater
OS6900-X48C6		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	denverton_cpucpld_v0b.02.0eh_20211124.jbc.updater
No CR	Description	Improved power down sequence when PSU shut down.
	CPLD File	os6900_x48c6_mainpldall_bp_v1.03.02.02h.jbc.updater
OS6900-X48C4E		
CRAOS8X-30098	Description	Fixed I2C lockup issue on CPU board. (Please refer to CRAOS8X-30098 for additional details)
	CPLD File	OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2e3228_20220322.updater
8.9R4 Release		
OS6900-X48C4E		
CRAOS8X-43968	Description	Fixed temperature error on OS6900-X48C4E (Hardware revision: 6) with a single power supply.
	CPLD File	updater_kit_8629 (version 2.15)

Notes:

1. Upgrading the CPLD on ONIE-based models using an updater kit is supported beginning with AOS Release 8.9.R03.
2. The updater kit contains all the necessary individual updater files.
3. CPLD versions are compatible with previous AOS releases. Downgrading to a previous AOS release is supported:
    a. Backup the configuration files from previous release.
    b. Upgrade to AOS Release 8.9.R03.
    c. Upgrade the CPLD.
    d. Downgrade to previous release. (ISSU is not supported when downgrading AOS)
    e. Restore the configuration.

Note: AOS must be upgraded to 8.10R2 prior to performing a CPLD upgrade using the updater kit.

ONIE-based platforms contain multiple CPLDs. The upgrade process will pick the correct updater file from the kit based on the platform and the CPLD type. The procedure will check for a version mismatch and upgrade the CPLD one at a time (i.e. Main board or CPU board). The CPLD will be upgraded one at a time so it may be necessary to run the command multiple times. If no upgrade is required, the command will display a message indicating there are no pending upgrades. See example below (file and product names will vary).

1. Download and extract the upgrade archive from the Service & Support website. In addition to the AOS images, the archive will also contain a CPLD upgrade kit, for example.

- CPLD Kit – updater_kit_8629

2. Ensure the configuration is certified and synchronized prior to upgrading the CPLD. It's recommended to have a console connection in case there are any issues during the CPLD upgrade procedure.

3. FTP (Binary) the updater kit to the **/flash** directory on the primary CMM.

4. Enter the following to upgrade the CPLD. Use the '**all**' parameter to upgrade each element in a VC, for example:

```
-> update fpga-cpld all 1/1 file updater_kit_8629
Starting CMM 1/1  FPGA Upgrade
CMM 1/1
starting onie update
Removing firmware update results: OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2f3238_20240315.updater
Staging firmware update: /flash/ OS6900_XC48C4E_MAIN_CPU_FAN_CPLD_2f3238_20240315.updater
onie update successful
Successfully updated
Reload required to activate new firmware.
```

5. If multiple CPLDs have to be upgraded the command must be run several times.
6. Once the CPLDs have been upgraded a manual reload is required. This will boot each of the units to "ONIE: Update ONIE" mode. **Note**: Do not press any keys while in ONIE mode.
7. The switch will update the CPLD and then reboot to the *Certified* directory. **Note**: The switch will not boot back to the last running directory.
8. OS6860N models (except U28) will then automatically power cycle. For all other models manually power cycle the units to refresh the CPLD image. The switch will then again boot back to the *Certified* directory.
9. Reload to the running-directory.

Appendix I: Fixed Problem Reports

The following problem reports were closed in this release.

CR/PR NUMBER	Description
Case: 00759867 *CRAOS8X-46448*	**Summary:** Local user account in switch is verified for TACACS+ authentication through TACACS+ server is active and when the user account is not present in TACACS+ server. This issue is noticed after upgrade to AOS 8.9R04. **Explanation:** Fix is provided to check the “local” user account only when TACACS+ server is down and fails over to the local server of the switch. Changes made in AOS 8.9R04 is reverted in AOS 8.10R02. 🔒 Click for Additional Information
Case: 00767420 *CRAOS8X-47184*	**Summary:** PMD is generated when BGP EVPN configured between OS6900 and 3rd party device. **Explanation:** The reason behind the switch generated PMD and reboots is after session establishment, rt3 routes processed in update message. It looks for local database whether the received routes are present or not. Initially, it is expected that the local database is empty. Null params are defined in swlog in case of local database is empty. This swlog process stopped due to referring to null params. Fix is given in swlog null parameters to handle the first time route updates properly. 🔒 Click for Additional Information
Case: 00772464 *CRAOS8X-47977*	**Summary:** Vulnerability impact analysis of CVE-2024-6119 in AOS 8.X switches. **Explanation:** The CVE is addressed in AOS 8.10R02 🔒 Click for Additional Information
Case: 00778380 *CRAOS8X-48807*	**Summary:** Nutanix plugin is not working as expected when multiple devices in same port. Truncating of outputs noticed in “show lldp remote-system” when more devices are connected behind Nutanix plug in enabled device. **Explanation:** Fix is provided to print the full output of LLDP remote-system behind Nutanix plug in enabled device. 🔒 Click for Additional Information
Case: 00752394 *CRAOS8X-45922*	**Summary:** Always the command “show spb isis interface <port or linkagg ID>” displays Adjacencies as “0” though SPB adjacent devices are connected. **Explanation:** The fix is available on AOS release 8.10R02. 🔒 Click for Additional Information
Case: 00754967 *CRAOS8X-46105*	**Summary:** The logs are printed as follows and there is no functional impact. mcipcd init ERR: : [pmApiGetPortState:2411] PMInit Not Done **Explanation:** "PMInit Not Done" error gets printed when the PmApiInitDone variable is NULL/0. MCIPCD

	process is getting started before the portmgrni. Fix is given to change the order of initialization. Click for Additional Information
Case: **00773702** *CRAOS8X-48602*	**Summary:** The switch management authentication (ASA) is successful with AOS 8.9.73.R01 and using ClearPass as Radius server, but it is getting rejected after the switch firmware is upgraded to AOS 8.9.94.R04 or AOS 8.10.102.R01. **Explanation:** In AOS 8.9R03, a service-type attribute in radius protocol packet for SSH authentication as UPAM server was expecting for CRAOS8X-41594. Fix was done similar to 6x and the value of service-type attribute was added as 2 PW_FRAMED_USER which was same for both SSH and 802.1x authentication. CPPM server couldn't differentiate between SSH and 802.1x authentication based on the service-type attribute and got failed. Fix is given to change the service-type attribute value as 6 (Administrative) for SSH authentication in RADIUS Access-Request packets towards RADIUS server. Click for Additional Information
Case: **00768706** *CRAOS8X-47330*	**Summary:** AOS 8X switch: OpenSSH version is revealed during scan. **Explanation:** OpenSSH version is revealed when performing Port Scan on AOS 8.X switch running 8.9R04. For security reasons, the version should be masked. The fix is available on 8.10R02. Click for Additional Information
Case: **00775446, 00766481, 00775915** *CRAOS8X-47107, CRAOS8X-48408*	**Summary:** Vulnerability check of CVE-2024-3596 for AOS 8X switches. The RADIUS Protocol, as specified in RFC 2865, is vulnerable to forgery attacks. A local attacker can exploit this by altering any valid response (such as Access-Accept, Access-Reject, or Access-Challenge) into another response type. This is achieved through a chosen-prefix collision attack targeting the MD5 Response Authenticator signature. **Explanation:** MAC authentication for wired users need to support the Attribute Value Pairs (AVP) message-authenticator attribute (80) in the RADIUS Access-Requests packets from AOS 8X switch to mitigate this attack. Fix is given in AOS 8.10R02. Click for Additional Information
Case: **00766022** *CRAOS8X-46869*	**Summary:** The following error message appears on the OS6360 console: WEBVIEW daemon ALRT message: +++ PHP Warning: Undefined array key "isSSO" in /var/webview/pages/index.php on line 147 **Explanation:** This warning message appears as 8.10.R01 is upgraded to PHP8. It doesn't cause any functional issues. Click for Additional Information

Case: **00764003** *CRAOS8X-46729*	**Summary:** Vulnerability analysis - CVE-2024-6387 for AOS 8X switches. **Explanation:** The CVE-2024-6387 is vulnerable, as the latest release (AOS 8.9.94R04) uses openSSH 9.6. As per the OpenSSH vulnerability (CVE-2024-6387), it is fixed in OpenSSH 9.8. Click for Additional Information
Case: **00769939** *CRAOS8X-46275*	**Summary:** OS6560P48Z16 fails to format the flash when using the Nrescue.img file. Switch stuck in Marvell mode. **Explanation:** The Switch's frequent access to the Flash (read/write) combined with power interruptions can lead to corruption in its Flash directories. This corruption can happen during bootup initialization or when power is lost. The issue stems from the flash driver, which manages the flash directories. This new software version introduces a defense mechanism designed to prevent and protect against flash corruption, along with an auto-recovery feature Click for Additional Information
Case: **00762535** *CRAOS8X-46679*	**Summary:** Switch reboots with PMD file when the CLI command "show ip redist-routes" is performed. **Explanation:** For profile low, the routing capabilities are restricted and by default, memory is not allocated. Hence accessing the IprmEnv for profile low was causing the crash. The changes were done appropriately to display the proper INFO message for "show ip redist-routes" CLI in profile low. The fix for this issue will be included in 8.10.R02 GA. Click for Additional Information
Case: **00765353** *CRAOS8X-46883*	**Summary:** The error "ERROR: Unable to retrieve VFC snapshot" displayed when performing show commands. **Explanation:** The issue is due to the VFC MIP socket doesn't have TCP keep alive. During the issue state, the MIP_GATEWAY TCP connection got lost with the VFCM. This caused the snapshot request to not be forwarded to VFCM. VFC can't detect the event to initiate reconnection when disconnection occurs. The changes made upon the reconnection mechanism on the VFCM with the MIP_GATEWAY and to setting the keep-alive for the socket. The fix for this issue will be included in 8.10.R02 GA. Click for Additional Information
Case: **00774243** *CRAOS8X-47111*	**Summary:** The device MAC address is not learnt on NULL-SAP port in SPB BEB switches in AOS 8.X switches such as OS6900-C32E and 2 OS6900-V48C8. Below logs were noticed in switch logs: swlogd tcamni main ERR: : [tcDbError:227] : tnDbTcamResourcesEntryInsert:1203 Database error 19, UNIQUE constraint failed: TnTcamResources.AppGroupId, TnTcamResources.AppId, TnTcamResources.ResourceId, TnTcamResources swlogd tcamni main ERR: : [tnHandleRuleCommitDel:3162] : tcDbTcRuleEntry exist in non committed state (TCAM_RET_NOT_FOUND) swlogd tcamni main ERR: : [tnApiRuleReqHandle:873] : TCAM_RET_NOT_FOUND **Explanation:** This issue is caused by incorrect TCAM provisioning for NULL-SAP ports and the fix for this issue is available in AOS 8.10R02.

	Click for Additional Information
Case: **00738201** *CRAOS8X-44207*	**Summary:** Learned Port Security (LPS) is not working, and ping is successful between Filtered MAC-address device to Bridged MAC-address device. **Explanation:** This is due to in the hardware register PROTOCOL_PKT_CONTROL, the bit ARP_REQUEST_TO_CPU=1 is set. Due to which, the packets are reaching the CPU and ping is working. The code changes were made to set the ARP_REQUEST_TO_CPU=0 and the issue is fixed in AOS 8.10R02. Click for Additional Information
Case: **00741438** *CRAOS8X-45422*	**Summary:** The DDM value displays as "0" for input and output for channel ports 2/1/1A-D in AOS 8.X switches **Explanation:** The root cause is due to the channel down, and it reports the Input, Output power values as '0' for all the channels. If any one of the channel ports is down, still the Input, Output value is 0 in ddm output. The code changes have been implemented to ensure that the transmit (TX) and receive (RX) power are set to '0' only for the specific channel (A, B, C, or D) is down rather than all channels of that port. For example, if Channel A (2/1/1A) is down, we will set the TX and RX power to '0' only for Channel A, while Channels B, C, and D will continue to display their expected power values. The fix is available from AOS 8.10R02. Click for Additional Information
Case: **00761754** *CRAOS8X-46739*	**Summary:** Unable to configure the sap port range for the same service. When configuring a sap for range of ports, getting error: SW3 service 1000 sap port 1/1/4-10:0 ERROR: Invalid interface number **Explanation:** The code changes have been implemented to configure the sap port range for the same service. The fix for this issue is available in 8.10.R02 GA. Click for Additional Information
Case: **00768425** *CRAOS8X-47258*	**Summary:** Unable to take backup of the Yukon models of 6900 switches from OV2500. **Explanation:** This is because Yukon model switches, such as the OS6900-X24, do not have multiple microcode packages like other switch models. However, the switch(os6900-X24) was attempting to fetch a microcode package, and since no additional packages were available, it displayed "unknown." The issue is fixed in 8.10.R02 GA. Click for Additional Information
Case: **00757340** *CRAOS8X-46552*	**Summary:** Mac-ping loss between OS9900 and OS6860N switches, despite no issue with SPB adjacency **Explanation**: It is identified that the first packet will be sent using "multicast-send-API" and the rest were

	sent using "unicast-send-API". The packet sent from the mcast API is not egressed out of the switch. Fix in 8.10.R02. Click for Additional Information
Case: **00747288** *CRAOS8X-45725*	**Summary**: The MACSEC feature on the 6465 switch cannot be activated when the switch port status is down. However, MACSEC activation will be successful if the switch port status is kept UP. **Explanation**: A fix has been implemented in AOS 8.10.R02 to correct the activation method of the MACSEC feature. It is no longer mandatory for the link to be in an UP state when enabling MACSEC. Click for Additional Information
Case: **00764512** *CRAOS8X-47179*	**Summary**: Configured the SPB domain with inline routing on the VC of a 6x6900 switch and applied QoS policies to drop packets destined for the switch's IP address; however, these packets were not dropped. **Explanation**: A fix has been implemented in AOS 8.10.R02 for the specific policy configuration regarding packets destined for the switch via SAP. These packets, which are sent to the CPU, will have their QoS classification handled by the software, and will be dropped according to the QoS configuration. Click for Additional Information
Case: **00747922** *CRAOS8X-45270*	**Summary:** The OS6465T-P12 switch fails to retain the date when powered off for 20 minutes or longer. When it is powered back on, the date resets to January 1, 1970. This issue caused an authentication failure when the switch was required to function as a Dot1x supplicant. **Explanation:** A fix has been implemented in AOS 8.10.R02 for the OS6465 switch to update the time in NVRAM, allowing the switch to use the stored time during booting. Click for Additional Information
Case: **00772410** *CRAOS8X-47703*	**Summary:** Stack of 4 OS6900-V48C8 multiple 25G VFL Interfaces bouncing and unable to change to FEC FC on the fly **Explanation**: VFL Interface Bouncing using 25G LR SPF, Stack of 4 OS6900-V48C8 multiple 25G VFL Interfaces keep bouncing using 8.8.R02. When set the interfaces FEC to FC. It shows that the port is configured as FC, but the field is operation field is still empty. So, when configured FC correctly and then it will bounce like crazy. When change FEC to FC or change FEC to disable didn't take effective. Click for Additional Information
Case: **00774783** *CRAOS8X-48052*	**Summary:** OS6465: User unable to access the switch via SSH, Telnet, and HTTPS with 8.10.102.R01 when using "Automatic Remote Config' **Explanation:** OS6465-User-unable-to-access-the-switch-via-SSH-Telnet-and-HTTPS-with-8-10-102-R01 the user is unable to access the switch via SSH, Telnet, and HTTPS.

	Click for Additional Information
Case: **00774846** *CRAOS8X-48100*	**Summary:** OS6560E-P48Z16: VLAN 1 qtagged inserted into the ARP reply from the ASIC 1 ports causing ping to fail on VLAN 1 port 2/1/24 and 1/1/33 **Explanation:** ASIC 1 has the following ports mapped: Device-1 user ports: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 33, 34, 35, 36 And all the ports that map to ASIC one all have the same problem where an 802.1q tag of VLAN 1 is inserted into the ARP packets, which is wrong. Click for Additional Information
Case: **00713498** *CRAOS8X-44063*	**Summary:** Enhanced protection against flash corruption during power loss **Explanation**: Improvements have been made to enhance protection against corruption caused by power loss. Click for Additional Information
Case: **00764519** *CRAOS8X-46768*	**Summary:** IPv6 QoS Policy Rules Not Working **Explanation**: Switch wasn't respecting the precedence of rules Click for Additional Information
Case: **00773159** *CRAOS8X-47786*	**Summary:** TCAM error when trying to change QoS config of VC **Explanation**: This update avoids the CLI hang, and adds more verbose error messages to help with troubleshooting Click for Additional Information
Case: **00782235** *CRAOS8X-49175*	**Summary:** Inserting SFP-Gig-T in a port brings down another port on OS99-XNI-U48 **Explanation**: Resolved port-mapping issue when SFP-Gig-T is inserted Click for Additional Information
Case: **00740222** *CRAOS8X-44508*	**Summary:** Clients connected to the OS6465 and OS6560 switch stopped getting IPV6 address via DHCPV6. **Explanation**: If the switch is configured with IPV6 multicast, the IPV6 packet is trapped to CPU and send to IPMS module and then to ip6ni. The ip6ni then drops the packet and this is the reason for DHCPV6 packet not been forwarded.

	Click for Additional Information
Case: **00754215** *CRAOS8X-45835*	**Summary:** In OS6570M-U28 switch, on port 1/1/25-28 the 10GIG copper DAC negotiate 1000Mbps even when the peer port is 10000Mbps. **Explanation:** This issue is limited to Copper SFP and not seen with fiber. With the ports in issue state, if the copper DAC in the ports 1/1/25-28 is physically toggled or if the switch is reloaded, then the link would go DOWN. User has to admin toggle the port with copper DAC to link UP. Click for Additional Information
Case: **00757789** *CRAOS8X-46266*	**Summary:** OS6900-X40 switch frequently printing the bcd arp ALRM in the switch console and the swlogs. **Explanation:** The information printed by the switch in "bcd arp ALRM message" is not informative. It is required to configured debug level logs to understand the issue. In the fixed microcode the bcd arp ALARM would be more informative. Click for Additional Information
Case: **00766904** *CRAOS8X-47096*	**Summary:** One of the chassis reloaded in a VC of 3 X OS6560-P48Z16 for unknown reason. **Explanation:** Enhancements done to log kernel crashes. Click for Additional Information
Case: **00766979** *CRAOS8X-47095*	**Summary:** OS6560-P48Z16 does not increment the "Packet Identifier" value in the RADIUS Access-Request packets and the value is always stuck with 0. **Explanation:** This issue is mostly seen during EAP-TLS auth, which involves several "Access-Request" and "Access-Challenge" packet exchange. For every "Access-Request", the AOS switch has to increment the "Packet Identifier" value; however, the value is mostly stuck with 0. Click for Additional Information
Case: **00767604** *CRAOS8X-47097*	**Summary:** After executing the command "write memory flash-synchro", the OS6900-V48C8 switch generated ERROR: no answer received (timeout)-18 (CLI-mip_msg_nowait_response) **Explanation:** The delay in sending "TRAPID_lnkaggPortLeave" and "TRAPID_linkDown" makes the trap handling overloaded. Switch processing too many TRAP requests leads to trapmgr been hanging and it cannot handle further requests from configmgr any more, leading to the ERROR. Click for Additional Information
Case: **00767585** *CRAOS8X-47102*	**Summary:** In OS6900-X48C6 switch, the LACPDU packets are forwarded by the switch to service access ports. This triggered linkagg flaps on several switches. **Explanation:** When null sap is configured, the service manager triggers a Tcam rule entry creation in

	ipvpn_null-sap resource for handling untagged traffic. Hence the initial LACP PDU's are tunneled through other member ports/linkaggs of the sap. Click for Additional Information
Case: **00767612** *CRAOS8X-47098*	**Summary:** OS6900-V48C8 switch frequently generated "[ERROR] FUNCTION trap_system_free LINE 305" in the swlogs. **Explanation:** As per design, ALL traps TRAPID_lnkaggPortLeave and TRAPID_linkDown are delayed 0.25s when being sent out. This makes buffer increased faster when receiving TRAPID_lnkaggPortLeave and TRAPID_linkDown requests, and makes the buffer running out. Click for Additional Information
Case: **00743556** *CRAOS8X-44561*	**Summary:** Increase debug level for swlog appid ipni causes a high CPU spike **Explanation**: Some internal port retrieval attempts are failing, and as the process continuously retries, the CPU is being utilized for each attempt. This repeated retrieval process leads to high CPU usage. All 8X switches are concerned and could face this starting from 8.9R01 Click for Additional Information
Case: **00761324** *CRAOS8X-46576*	**Summary:** sw-supp-secure-mode featureis not applied when using unp template **Explanation:** The sw-supp-secure-mode option works when applied directly to a port, but when used in a template, the port where the template is applied does not have the option enabled. Click for Additional Information
Case: **00748260** CRAOS8X-49488	**Summary:** 8x switch as .1x supplicant keeps "trust-tag" after port goes down again **Explanation:** When the 6560-supplicant switch is replaced by the 6360 non-supplicant switch, the 6860-authenticator should detect that the 6360 is not an authenticated supplicant and should place the connected user (User B) in a blocking state. However, the 6860-authenticator fails to do this, and instead, User B is still learned with a trust tag and granted access, even though the 6360 non-supplicant switch should not have access. Click for Additional Information
Case: **00741185** CRAOS8X-44401	**Summary:** OS6900: SPB Adjacency issue. **Explanation:** The SPB nodes connected to Master unit in the VC were getting lost and the traffic that should pass through Master unit where more nodes are connected losing the communication which is leading to partial outage of this part of network for 300 seconds. Click for Additional Information
Case: **00760585** *CRAOS8X-46571*	**Summary:** OS6900: LACP link flap issue on the SAP ports. "buffer overflow detected". **Explanation:** Due to linkagg issue on OS6900 switch running 8.9.221.R03. To troubleshoot the seen problem tried enabling linkagg debugs however noticed buffer overflow detected.

	OS6900->swlog appid *** buffer overflow detected ***: clicomp terminated Click for Additional Information
Case: **00770079** *CRAOS8X-47448*	**Summary:** OS6860N-P48Z: Following reload, all UNP ports are blocked, with Failure Reason as "SPB Service-Id mismatch - Block" **Explanation:** AG CMM module crashes after reloading, causing all the UNP ports to go into Blocking state. Click for Additional Information
Case: **00776258** *CRAOS8X-49112*	**Summary:** OS6465T-12: Packets with same source and destination IP address are dropped in VLAN Stacking **Explanation:** OS6465T-12: Packets with same source and destination IP address are dropped in VLAN Stacking The results in discarding of BFD packets. Click for Additional Information
Case: **00722591** *CRAOS8X-42412*	**Summary:** OS6900-V72: "IfOutErrors" are displayed for linkagg but not for the physical interfaces **Explanation:** "IfOutErrors" are displayed for linkagg but not for the physical interfaces Click for Additional Information
Case: **00750376** *CRAOS8X-45464*	**Summary:** OS6865-P16X- Not able to create SAP port configuration with error “ERROR: Invalid Port State TAGGED”. **Explanation:** Set the port state to TAGGED for spb port configuration and set the port state to FIXED for un-configuring the spb port when VPAs are not associated to the port. Click for Additional Information
Case: **00766248** *CRAOS8X-46896*	**Summary:** OS6900 linkagg port TCAM Error. **Explanation:** The LACP packets are not trapped to the CPU;Stale entries created in TCAM due to overlapping port pair combinations in the switch, leading to lacp pdus not getting trapped to CPU and thus member ports not able to join the linkagg. Click for Additional Information
Case: **00759141** *CRAOS8X-46517 / CRAOS8X-44903*	**Summary:** In OS9900 NTP client configuration is disabled once the CMM failover is done. **Explanation:** During the failover test of the CMM in the OS9900 VC, CMMB has the "ntp client admin-state enable" configuration. However, when running the "show ntp client" command, the switch reports that the NTP client is disabled. Click for Additional Information
Case: **00777358**	**Summary:** The switch management authentication is successful with AOS 8.9.73.R01 using ClearPass as

CRAOS8X-48541 / CRAOS8X-47818	the RADIUS server. However, after upgrading the switch firmware to AOS 8.9.94.R04 the authentication is being rejected. **Explanation:** The issue is caused by the introduction of a new service-type field, "Framed-User (2)," in the RADIUS access request message. The service-type attribute was set to 2 (PW_FRAMED_USER), which is used for both SSH and 802.1X authentication. Click for Additional Information
Case: 00756527 *CRAOS8X-46450*	**Summary:** The MAC address table on the OS6560 switches is not updating correctly. On the port connected to the access point (AP), the switch continues to display the MAC address of a client that has already been disconnected from the AP. **Explanation:** The switch port initially learns the client's MAC address from the connected access point (AP). After the client disconnects from the AP, the MAC address remains in the switch port's table until the ageing timeout expires, at which point the entry should be removed. In the case of the reported issue, the MAC address persists even after the ageing timeout has passed. Click for Additional Information
Case: 00755876 *CRAOS8X-46044*	**Summary:** Logging clarification for UNP blocking for mismatched VLAN **Explanation:** If a packet arrives on a UNP port with a VLAN tag that does not match the VLAN configured in the UNP Profile, the port will be placed into a blocking status. 8.10.R02 adds the following log message to show this block reason, "agCmmAssignProfileToMac:3354 TagVlan [10] does not match the vlan [26] in profile [TestProfile]" Click for Additional Information
Case: 00766214 *CRAOS8X-46887*	**Summary:** The following log appears in the console every 30 seconds after upgrading to 8.10.R01:"lldpCmm Mgr INFO message: +++ AP device[with devType=4] detected on UNP port(1/1/9). Send LLDP event" **Explanation:** This log is displayed when an LLDP packet is received from a Stellar AP 1321. It was been moved to debug3 in 8.10.R02 Click for Additional Information
Case: 00766684 *CRAOS8X-47104*	**Summary:** Switches are are replying "Not in time window" from an SNMP walk attempt **Explanation:** There is a variable used for determining SNMP engine time that needs to be in sync with another variable that notes if the switch has rebooted. The mechanism for determining switch reboots was based on system time such that if the time on the switch was moved backwards, the variable would update. This would put the two SNMP Engine variables out of sync causing the issue. Click for Additional Information
Case: 00769379 *CRAOS8X-47426*	**Summary:** Switch not learning MAC addresses on Null-SAP ports **Explanation:** This issue is caused by incorrect TCAM provisioning.

	Each port is "provisioned" in TCAM via "TCAM Rules". Typically, this is done via configuration and the properties of each port do not change frequently. SAP is special in that it will dynamically change that provisioning. Incorrect TCAM provisioning can occur if two interfaces are configured for a null SAP that are 16 interfaces apart, i.e. 1/1/1 and 1/1/17 or 5/1/10 and 5/1/26. These SAPs do not need to be in the same service for the staling to occur, these interfaces can also be a part of Linkaggs. Click for Additional Information
Case: **00767657** *CRAOS8X-47111*	**Summary**: Null-SAP ports tunneling LACP packets **Explanation**: This issue is caused by incorrect TCAM provisioning. Each port is "provisioned" in TCAM via "TCAM Rules". Typically, this is done via configuration and the properties of each port do not change frequently. SAP is special in that it will dynamically change that provisioning. In 8.9.R04, it is possible for null-SAP entries (any SAP using ':0' such as "service 1 sap linkagg 108:0"), to become stale where the configuration of SAP persists even after the SAP should be disconnected. A port with a SAP configuration would tunnel traffic, and a port without SAP configuration would process traffic. This applies to LACP traffic as well. If a port with stale SAP configuration receives LACP traffic, it will be tunneled rather than processed. Notably, it appears that this staling is resolved after some time, so not all LACP packets are tunneled all the time. The issue only occurs briefly after a LinkAgg has flapped. This issue with stale null-SAP entries occurs if two interfaces are configured for SAP that are 16 interfaces apart, i.e. 1/1/1 and 1/1/17 or 5/1/10 and 5/1/26. These SAPs do not need to be in the same service for an issue to occur. Click for Additional Information
Case: **00755476** *CRAOS8X-46039*	**Summary:** The packets are dropped on DHCP-Snooping and IP-Source filter enabled ports. **Explanation**: The issue is due to erroneously matching the rule ID of the working client with the client who sent the DHCP release. This causes the working client entry to be removed from the database thus rejecting the traffic from that client. Click for Additional Information
Case: **00753035** *CRAOS8X-45702*	**Summary:** The GTTS tunnel is not formed after reboot when the default route is present to reach the Far end IP. **Explanation:** The issue is seen only when the default route or the less specific routes are used. To reach the far-end IP during the reboot. A workaround is to configure /32 route to the gateway. The issue is fixed in AOS 8.10 R01 MR. Click for Additional Information

Case: **00739174** CRAOS8X-45679	Summary: The front panel port stays on oS6900-X48C6 after a VC split even though the VCSP has been activated. **Explanation:** When the VCSP is active after Vc split happens, the front panel ports should go down. However the port stays UP. The issue is seen when the SFP-GIF-T is used on the front panel.This is fixed in AOS 8.10 R02 Click for Additional Information
Case: **00764012** CRAOS8X-46749	**Summary:** Port range is allowed when creating SAP ports but not allowed when assigning a given service to SAP ports. **Explanation**: A fix has been applied to 8.10.109.R01 to allow for using a port range when assigning a service to a range of contiguous ports. Click for Additional Information
Case: **00751891** CRAOS8X-45840	**Summary:** Link does not come UP when copper SFP-1G-T is connected in 6560-P24Z8 ports 1/1/25-26. **Explanation:** When a 1-GIG-T copper SFP (single speed) plugged in (interface 26) without establishing the link, gives an invalid interrupt because of which valid link status change from the other interface (interface 25) is not processed. However, when interface 26 is up with link, interface 25 link connection also works fine. This is fixed in AOS 8.10 R01 MR Click for Additional Information
Case: **00754484** **CRAOS8X-46173**	**Summary:** UNP user device entry is not removed from UNP table and MAC-learning table though user is disconnected from IP phone. **Explanation**: Fix is provided to clear the MAC-table and UNP table after MAC-aging time (twice the MAC-aging default time) once the user device is disconnected from IP phone on UNP port. Click for Additional Information
Case: **00750963** *CRAOS8X-45430*	**Summary:** SNMPwalk result for OID dot1qTpFdbPort shows same index value for all the MAC addresses on the port **Explanation**: The output for dot1qTpFdbPort SNMP OID on the switch is showing the same VLAN ID (1) for all MAC addresses associated with a port, instead of displaying the individual VLAN ID for each MAC address. Click for Additional Information
Case: **00758844** *CRAOS8X-46311*	**Summary:** Console logs of slave chassis are displayed even with console logging off. **Explanation:** In a Virtual Chassis (VC) setup with two or more switches, the console logs from the member (or slave) chassis are displayed on the master chassis, even if console logging is disabled.

	🔒 Click for Additional Information
Case: **00777833** *CRAOS8X-48555*	**Summary:** Show Port-security port [port number] command shows "Check PortCB on [number]" **Explanation:** While verifying the port-security configuration on a newly set up UNP port using the command "show port-security port 2/1/44", the following error message is displayed: show port-security port 2/1/44 Check PortCB on 131115 Error disappears after reconfiguring port-security on the port. 🔒 Click for Additional Information
Case: **00777894** *CRAOS8X-48481*	**Summary:** Error Message during write memory "diff: can't stat '/tmp/tmp.4jbkLb/onie/initrd.ale': No such file or directory". **Explanation:** Error message while doing write memory: write memory flash-synchro File /flash/working/vcsetup.cfg replaced. File /flash/working/vcboot.cfg replaced. Please wait... diff: can't stat '/tmp/tmp.4jbkLb/onie/initrd.ale': No such file or directory diff: can't stat '/tmp/tmp.4jbkLb/onie/ale_rescue.sh': No such file or directory Regardless of the error, write mem flash-sync works fine. ***Note:*** This error is observed after upgrading the switch from AOS version 8.9R04 to 8.10R01, or the switch is reloaded with AOS 8.10R01. It occurs when running the write memory flash-synchro command. The error indicates that specific temporary files (initrd.ale and ale_rescue.sh) in the /tmp/tmp.4jbkLb/onie/ directory are missing. 🔒 Click for Additional Information
Case: **000077703** *CRAOS8X-47097*	**Summary:** Errors During show configuration snapshot and write memory flash-sync **Explanation:** Following errors are seen during migration of links from old switch to the new switch: Show configuration snapshot ERROR: System is busy. Please try later. (1008) ERROR: Unable to retrieve TRAP snapshot. write memory flash-sync ERROR: no answer received (timeout)-18 (CLI-mip_msg_nowait_response) 🔒 Click for Additional Information
Case: **00754623** *CRAOS8X-46129*	**Summary:** BFD is not re-establishing after a failure. **Explanation:** When an OmniSwitch is peered with a Juniper device BFD does not re-establish after a failure between the 2 devices. BFD must be toggled on the ALE side in order to re-establish the BFD session. 🔒 Click for Additional Information
Case: **00775101** *CRAOS8X-48239*	**Summary:** IPv6 routes are going into software on OS6900-V48C8 when in router mode but not exceeding the route limit.

	Explanation: This pivot schema for router mode has been increased in order to allow for more non-contiguous routes to be inserted into hardware. 🔒 Click for Additional Information

Appendix J: Installing/Removing Packages

The package manager provides a generic infrastructure to install AOS or non-AOS third party Debian packages and patches. The following packages are supported. The package files are kept in the **flash/working/pkg** directory or can be downloaded from the Service & Support website.

Package	Package Description
uos-mrp-v1.deb nos-mrp-v1.deb	MRP Application
*-ams-v#.deb *-ams-apps-v#.deb	AOS Micro Services Application
uosn-mpls-v4.deb uosn-sitemgr-v3.deb uosn-siteend-v2.deb yos-mpls-v4.deb yos-sitemgr-v3.deb yos-siteend-v2.deb	MPLS Application and Licensing
yos-nutanix-v3.deb	Nutanix Prism Plug-in Package
ovng-agent-v.1.10.deb	OmniVista Cirrus 10
kaos-sitemgr-v3.deb kaos-siteend-v2.deb	Licensing for SW-PERF for 6870
- If a package is not committed it can result in image validation errors when trying to reload the switch. - Some packages are included as part of the AOS release and do not have to be installed separately. - Applications should be stopped prior to upgrading a package.	

Installing Packages

Verify the package prior to install. Then install and commit the package to complete the installation. For example:

```
-> pkgmgr verify nos-mrp-v1.deb
  Verifying MD5 checksum.. OK
-> pkgmgr install nos-mrp-v1.deb
-> write memory
-> show pkgmgr

Legend: (+) indicates package is not saved across reboot

        (*) indicates packages will be installed or removed after reload

Name                Version           Status              Install Script

-------------+--------------------+------------------+-----------------------------    ams
default               installed          default
ams-apps      default               installed          default
mrp           8.7.R03-xxx           installed      /flash/working/pkg/mrp/install.sh
```

Removing Packages

Find the name of the package to be removed using the **show pkgmgr** command, then remove and commit the package to complete the removal. Remove the Debian installation file. For example:

```
-> pkgmgr remove mrp
Purging mrp (8.7.R03-xxx)...
Removing package mrp.. OK
Write memory is required complete package mrp removal
-> write memory
Package(s) Committed

-> show pkgmgr
Legend: (+) indicates package is not saved across reboot
        (*) indicates packages will be installed or removed after reload
Name                Version           Status              Install Script
--------------+--------------------+------------------+--------------------------------
  ams           default               installed          default
  ams-apps      default               installed          default
  mrp         8.7.R03-xxx           removed            /flash/working/pkg/mrp/install.sh
```

Remove the Debian package installation file. For example:

```
-> rm /flash/working/pkg/nos-mrp-v#.deb
```

AOS Upgrade with Encrypted Passwords

AMS

The ams-broker.cfg configuration file for AMS contains plain text passwords. The passwords can be stored as encrypted beginning with the 8.7R1 release. Follow the steps below prior to upgrading to 8.7R1 or later release to store encrypted passwords.

1. Remove *ams-broker.cfg* file present under path /flash/<running-directory>/pkg/ams/ prior to upgrading AOS.
2. This will remove the broker configuration which must be re-configured after the upgrade.
3. Remove this file from each VC node.
4. Upgrade the switch.
5. Once the switch comes up after the upgrade, the password present under/flash/<running-directory>/pkg/ams/ams-broker.cfg file will be encrypted.

IoT-Profiler

The ovbroker.cfg configuration file for AMS-APPS/IoT-Profiler contains plain text passwords. The passwords can be stored as encrypted beginning with the 8.7R1 release. Follow the steps below prior to upgrading to 8.7R1 or later release to store encrypted passwords.

1. Remove the *install.sh* file present under path /flash/<running-directory>/pkg/ams-apps/ for AMS-APPS prior to upgrading AOS.
2. Remove this file from each VC node.
3. Upgrade the switch.
4. Once the switch comes up after the upgrade, the password present under/flash/<running-directory>/pkg/ams-apps/ovbroker.cfg file will be encrypted.

Appendix K: Fixed CVEs

The following CVE CRs were fixed in this release.

CVE CRs	CVE	CVSS

CRAOS8X-46556	CVE-2024-6387	8.1
CRAOS8X-46660	CVE-2024-3596	9 (some list as 7.5)