



Alcatel-Lucent OmniAccess Stellar Access Point

Broadcast and multicast optimisation

Application note

OmniVista UPAM and Palo Alto Networks User-ID Integration Guide

Table of Contents

Prerequisites	3
Executive summary	3
Multicast	4
Challenges	4
Multicast optimisation	4
Configuration	5
Broadcast	11
Broadcast key rotation	11
Address Resolution Protocol (ARP) filtering	12
All protocols filtering.....	13
Conclusion.....	16

Prerequisites

- Alcatel-Lucent OmniVista® Cirrus Network Management as a Service R10.3
- Alcatel-Lucent OmniVista Cirrus 4.7.1 GA
- Alcatel-Lucent OmniVista 2500 Network Management System 4.7R1 GA
- Alcatel-Lucent OmniAccess® Stellar Access Point (Wi-Fi 5 or 6/E)
- AWOS 4.0.5.3052

Executive summary

Multicast and broadcast are transmission modes used to send data to multiple recipients at the same time, but they have significant differences:

- Broadcast sends data to all machines on the network, while multicast sends data to a selected group of machines
- Multicast is more efficient than broadcast because it avoids saturating the network with copies of identical data. Instead, the data is sent only once to a select group of machines.

However, there are challenges associated with the extensive use of multicast and broadcast in wireless networks. Here are some of the main problems:

- Bandwidth consumption: Multicast and broadcast can consume a large amount of bandwidth on the network, especially if many devices are connected to the network. This can lead to network saturation and decreased performance.
- Latency: Extensive use of multicast and broadcast can also lead to increased latency on the network, as many copies of data are sent to multiple recipients simultaneously
- Power Usage: Receiving multicast and broadcast can also result in increased power usage on wireless devices, which can impact battery life
- Security: Multicast and broadcast can also pose security concerns, as they can be easily intercepted and exploited by malicious individuals

This Application Note is designed to help users overcome these issues. Users will discover multiple techniques to improve network efficiency through explanations of features and recommendations.

Multicast

Multicast is a method of delivering identical data to multiple recipients simultaneously, without the source having to produce duplicates for each receiver. Unlike broadcast traffic that is sent to every device regardless of their interest, multicast enables receivers to opt-in to the traffic they desire. Consequently, this approach enhances efficiency because data is transmitted only once and minimises overhead (unintended receivers do not receive the data). Multicast is generally used in real-time data transmission, multimedia conferencing services and IPTV.

Challenges

Resources

One of the characteristics of multicast transmission over Wi-Fi is that every station must be configured to wake up to receive the multicast frame, even though the received packet may ultimately be discarded. This process can have a significant effect on the power consumption by the multicast receiver station. As well, for the Access Point, the CPU is highly solicited.

Wireless

Wireless clients share a collision domain. Since multicast is a single transmission that must be received by all transmitted receivers, access points are forced to send this frame at the lowest common denominator parameters, to give receivers the best chance of receiving the transmission without interruption. While this is appropriate for small broadcast traffic such as beacons, it is not viable for high bandwidth applications.

Multicast traffic is sent at the DTIM interval. When a multicast frame is transmitted, all Wi-Fi clients must wake up to listen to the frame and discard it if they do not need it.

Battery-powered devices therefore remain awake much longer than necessary because if the DTIM interval is too long, the increased latency can impact real-time applications like video. But the lower the DTIM interval, the more often wireless clients must wake up.

However, there is a way to optimise multicast traffic wireless for the above constraints. This information will be provided in the Multicast Optimisation chapter.

Multicast optimisation

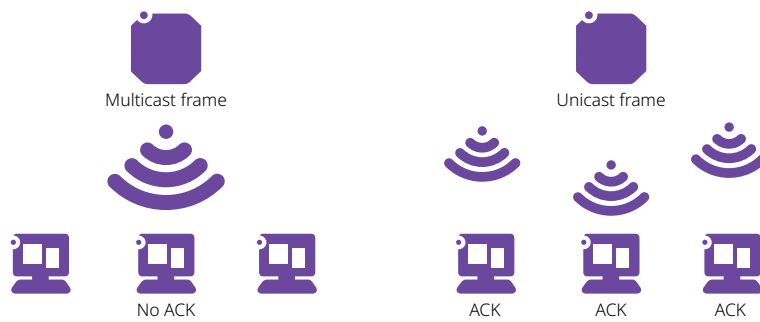
Multicast to unicast

Multicast to unicast conversion in a wireless network is a technique used to improve the efficiency of delivering multicast traffic to wireless clients. In a multicast transmission, a single data stream is sent to multiple recipients simultaneously. However, wireless clients have limited capabilities in processing multicast traffic, and it can be challenging to deliver the data reliably and efficiently to all clients.

To overcome this challenge, multicast to unicast conversion is used. In this technique, the multicast traffic is converted into unicast traffic, which is sent separately to each wireless client. Each client receives a dedicated copy of the data, ensuring that it is received reliably and efficiently without any congestion or delays.

By converting multicast traffic to unicast, the network can ensure that each client receives the data reliably and with minimal latency, improving the overall user experience.

In many situations, it's a good choice to use unicast instead of multicast over Wi-Fi. This avoids most of the problems specific to multicast over Wi-Fi, since the individual frames are then acknowledged and buffered for power-save clients in the way that unicast traffic normally operates.



IGMP snooping must be enabled

That is why it is more efficient for the “threshold” number of clients to convert multicast traffic to unicast traffic and send it directly to the destination (based on the IGMP snooping).

Configuration

AP Group configuration

There is a switch to enable “IGMP snooping” on the AP Group profile.

Miscellaneous	
Virtual IP Address ⓘ	1.1.1.1
Called Station ID	
IPv6 L3 Forwarding	☐ OFF
IGMP Snooping	☒ ON

When IGMP snooping is not enabled on AP, the multicast packets are forwarded to all downlink ports and ath (BSSID). However, if you enable the feature, the multicast packets are only forwarded to downlink ports and ath (BSSID) that are in the IGMP multicast table maintained by IGMP snooping.

SSID configuration

The configuration of multicast optimisation is per SSID, so different SSID may have different multicast optimisation options.

Multicast Optimization	☒ ENABLED
Multicast Based Channel Utilization	90 % v ^
Number Of Clients	6 v ^

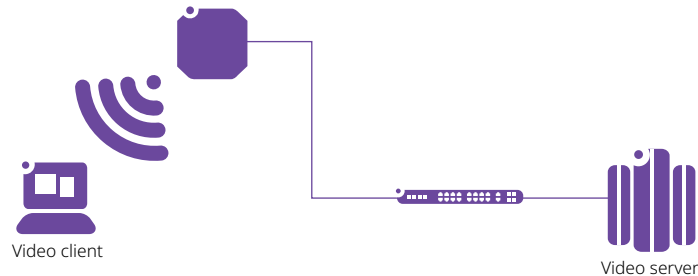
We use two thresholds: The number of clients and the Multicast Based Channel Utilisation. Once either of these thresholds is reached, the process of converting multicast to unicast will be stopped. It is important to note that these thresholds are in place solely to preserve the Access Point CPU.

Up to six clients is considered a good practice. When the multicast traffic has been requested by more clients, there is no longer a translation to unicast, and the traffic is multicast to the whole network.

Scenario 1

Context

This scenario demonstrates the optimisation of multicast flows over the air. Let's start by introducing the context of this scenario. We have a multimedia server and a client that will subscribe to a multicast stream. The server uses a wired connection, and the client is connected to the network using Wi-Fi. The client and server are on the same network segment.



Name	Mac Address	IP Address/CIDR
Video Server	00:50:56:8a:ab:0d	172.20.1.107/24
Video Client	0c:8b:fd:29:a1:d5	172.20.1.108/24

Multicast optimisation disabled

Now, let's analyse the behaviour of the access point if the "Multicast Optimisation" option is not activated. After capturing 802.11 frames on the OmniAccess Stellar Access Point (AP), we will look at the information displayed.

	Time	Source	Destination	Protocol	Length
	1920 6.466801	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1921 6.468078	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1922 6.469349	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1923 6.470686	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1985 6.702531	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1986 6.703833	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1990 6.711312	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444
	1996 6.726153	VMware_8a:ab:0d	IPv4mcast_09:09:09	802.11	1444

Frame 1920: 1444 bytes on wire (11552 bits), 1444 bytes captured (11552 bits) on interface 0
Ethernet II, Src: VMware_8a:ab:0d, Dst: IPv4mcast_09:09:09
802.11 radio information
PHY type: 802.11b (HR/DSSS) (4)
Short preamble: False
Data rate: 11.0 Mb/s
Channel: 11

In this screenshot we have two important pieces of information. First, we can see that the multicast traffic is propagated over the air (Destination: IPv4mcast_09:09:09). Additionally, we can see that the data rate is 11mb/s.

Multicast optimisation enabled

After enabling the “Multicast optimisation” feature, if we refer to the Configuration, we will see some useful information. We no longer see multicast destination traffic. Instead, we can see that the multicast traffic has been converted to unicast to the subscriber. Now, if we look at the “Data Rate”, we notice that the value is equal to 144mb/s.

	Time	Source	Destination	Protocol
14618	46.228844	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14611	46.214679	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14609	46.214314	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14566	46.026237	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14565	46.026229	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14564	46.026211	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14562	46.025624	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14511	45.804369	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11
14510	45.804361	VMware_8a:ab:0d	IntelCor_29:a1:d5	802.11

Frame 14618: 1450 bytes on wire (11600 bits), 1450 bytes captured (11600 bits) on 0, 1450 bytes captured (11600 bits) on 0, interface 0

Radiotap Header v0, Length 56 Scenario 2

802.11 radio information

PHY type: 802.11n (HT) (7) Context

MCS index: 15

Bandwidth: 20 MHz (0)

Short GI: True

Number of STBC streams: 0

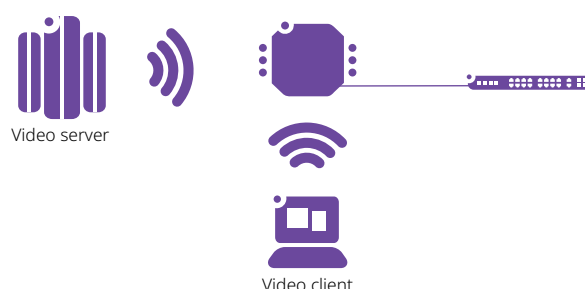
Data rate: 144,4 Mb/s

Channel: 11

Scenario 2

Context

In this scenario, we have a video server connected to the wireless network, along with a client also connected to the same network. The aim of this exercise is to analyse the behaviour of the OmniAccess Stellar AP in managing multicast traffic.



Name	MAC Address	IP Address/CIDR	VLAN
Video Server	0c:8b:fd:29:a1:d5	192.168.25.4/24	25
Video Client	64:bc:58:e7:84:39	192.168.25.5/24	25

The screenshot shows us that the multicast flow does not go through a unicast conversation process. Indeed, the multicast flow is propagated in the air without specific treatment.

Application note

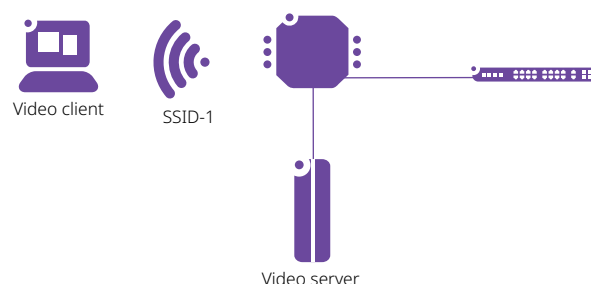
12 0.023621	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11
13 0.023631	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11
14 0.023640	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11
15 0.023650	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11
16 0.023659	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11
17 0.023670	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11
18 0.023679	IntelCor_29:a1:d5	IPv4mcast_01:01:16	802.11

> Frame 13: 1534 bytes on wire (12272 bits), 1534 bytes captured	0000
> Radiotap Header v0, Length 56	0010
> 802.11 radio information	0020
PHY type: 802.11n (HT) (7)	0030
MCS index: 14	0040
Bandwidth: 20 MHz (0)	0050
Short GI: True	0060
Number of STBC streams: 0	0070
Data rate: 130.0 Mb/s	0080
Channel: 11	0090
	00a0
	00b0

Scenario 3

Context

In this situation, we will be using an OmniAccess Stellar AP that was originally designed for the hospitality industry. Notably, this access point embeds unique features such as RJ-45 ports. In this scenario we will establish a connection between the video server and one of the ports on the OmniAccess Stellar AP. Subsequently, we will connect a wireless client to the SSID-1 network. Lastly, we will assess the access point's ability to manage the multicast flow.



Name	MAC Address	IP Address/CIDR	VLAN
Video Server	00:90:f5:ec:3a:69	192.168.35.5/24	35
Video Client	64:bc:58:e7:84:39	192.168.25.3/24	25

Based on the screenshot presented, it appears that the multicast stream has undergone a conversion process and is now in the form of unicast transmission.

829 4.956514	192.168.35.5	231.1.1.1	UDP
830 4.962803	192.168.35.5	231.1.1.1	UDP
831 4.969190	192.168.35.5	231.1.1.1	UDP
832 4.975472	192.168.35.5	231.1.1.1	UDP
833 4.981565	192.168.35.5	231.1.1.1	UDP
834 4.988155	192.168.35.5	231.1.1.1	UDP
835 4.994349	192.168.35.5	231.1.1.1	UDP
836 5.000389	192.168.35.5	231.1.1.1	UDP

Frame 841: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Alcatel-_ab:19:ad (e8:e7:32:ab:19:ad), Dst: IntelC
> Destination: IntelCor_e7:84:39 (64:bc:58:e7:84:39)
> Source: Alcatel-_ab:19:ad (e8:e7:32:ab:19:ad)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.35.5, Dst: 231.1.1.1
User Datagram Protocol, Src Port: 8888, Dst Port: 8888

Application note

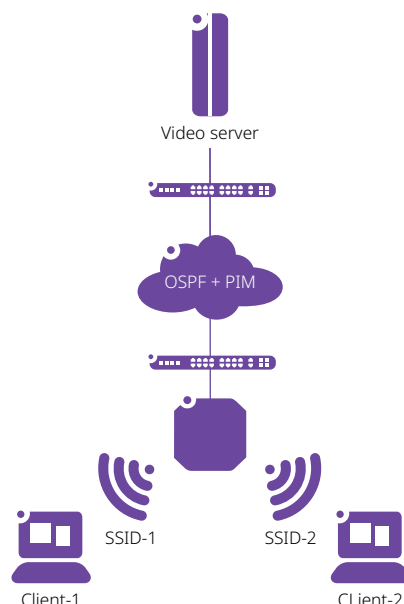
Alcatel-Lucent OmniAccess Stellar Access Point

Scenario 4

Context

The multicast optimisation feature is architecture-agnostic and can operate at both the Layer 2 and Layer 3 levels.

In this scenario, we have a video server and two clients connected to two different SSIDs, resulting in two distinct networks. To accomplish this, we used several protocols, including the implementation of a dynamic routing protocol like OSPF, as well as a multicast routing protocol such as PIM.



Name	MAC Address	IP Address/CIDR	VLAN
Video Server	00:50:56:8a:ab:0d	172.20.1.107/24	172
Client-1	44:01:bb:88:2a:b6	192.168.25.1/24	25
Client-2	44:01:bb:88:29:02	192.168.35.1/24	35

The above screenshot shows that the multicast traffic undergoes conversion to unicast, enabling it to be transmitted to two distinct clients located in VLAN 25 and 35, respectively.

Source	Destination	Protocol
Alcatel-_ab:19:ad	Shenzhen_88:2a:b6	802.11
Alcatel-_ab:19:ad	Shenzhen_88:2a:b6	802.11
Alcatel-_ab:19:ad	Shenzhen_88:2a:b6	802.11
Alcatel-_ab:19:ad	Shenzhen_88:2a:b6	802.11
Alcatel-_ab:19:ad	Shenzhen_88:2a:b6	802.11

Source	Destination	Protocol
Alcatel-_ab:19:ad	Shenzhen_88:29:02	802.11
Alcatel-_ab:19:ad	Shenzhen_88:29:02	802.11
Alcatel-_ab:19:ad	Shenzhen_88:29:02	802.11
Alcatel-_ab:19:ad	Shenzhen_88:29:02	802.11
Alcatel-_ab:19:ad	Shenzhen_88:29:02	802.11

With regard to the transmission speed, the screenshots below demonstrate a speed of 72.2 megabytes per second (MB/s).

Application note

Alcatel-Lucent OmniAccess Stellar Access Point

▼ 802.11 radio information
PHY type: 802.11n (HT) (7)
MCS index: 7
Bandwidth: 20 MHz (0)
Short GI: True
Number of STBC streams: 0
Data rate: 72.2 Mb/s

▼ 802.11 radio information
PHY type: 802.11n (HT) (7)
MCS index: 7
Bandwidth: 20 MHz (0)
Short GI: True
Number of STBC streams: 0
Data rate: 72.2 Mb/s

Following are the details pertaining to the access point connection used by Client-1 and Client-2. The previously identified speed of 72.2 megabytes per second (MB/s) is a direct outcome of the negotiation that took place between the clients and the OmniAccess Stellar AP.

```
C:\Users\admin>netsh wlan show interfaces

Il existe 1 interface sur le système :

Nom                : Wi-Fi
Description         : Realtek 8821CU Wireless LAN 802.11ac USB NIC
GUID               : 832f3425-39c3-4599-8511-c0316f05dc6a
Adresse physique    : 44:01:bb:88:2a:b6
Etat               : connecté
SSID               : MCAST_VLAN25
BSSID              : dc:08:56:0d:29:c2
Type de réseau     : Infrastructure
Type de radio      : 802.11n
Authentification   : WPA2 - Personnel
Chiffrement        : CCMP
Mode de connexion  : Profil
Canal              : 11
Réception (Mbits/s) : 72.2
Transmission (Mbits/s) : 72.2
Signal             : 100%
Profil             : MCAST_VLAN25
```



```
C:\Users\admin>netsh wlan show interfaces

Il existe 1 interface sur le système :

Nom                : Wi-Fi
Description         : Realtek 8821CU Wireless LAN 802.11ac USB NIC
GUID               : 832f3425-39c3-4599-8511-c0316f05dc6a
Adresse physique    : 44:01:bb:88:29:02
Etat               : connecte
SSID               : MCAST_VLAN35
BSSID              : dc:08:56:0d:29:c3
Type de réseau     : Infrastructure
Type de radio      : 802.11n
Authentification   : WPA2 - Personnel
Chiffrement        : CCMP
Mode de connexion  : Profil
Canal              : 11
Réception (Mbits/s) : 72.2
Transmission (Mbits/s) : 72.2
Signal             : 100%
Profil             : MCAST_VLAN35
```

In summary

Multicast optimisation plays a crucial role in preserving airtime by efficiently managing network resources. With this optimisation technique, multicast packets are transmitted as unicast messages, enhancing their delivery efficiency.

To ensure the smooth CPU operation, specific thresholds are established. Within these thresholds, optimisation is carried out, maximising performance while maintaining AP stability.

In cases where IGMP snooping is disabled on the AP, multicast packets are indiscriminately forwarded to all downlink ports and the ath (BSSID) interface. However, when IGMP snooping is enabled on the AP, multicast packets are selectively forwarded only to downlink ports and ath (BSSID) interfaces that are listed in the IGMP multicast table managed by IGMP snooping.

When multicast optimisation is not enabled for a particular SSID associated with an ath/BSSID, multicast packets are distributed to all connected clients while preserving the multicast destination MAC address. When multicast optimisation is enabled for the same SSID and ath/BSSID, multicast packets are individually sent to each associated client using a unicast destination MAC address.

In Wi-Fi 5 AP models, the multicast optimisation function operates within certain limitations determined by factors such as channel utilisation and the number of clients. Once the channel utilisation or client threshold is reached, the conversion of multicast to unicast transmission ceases. However, in Wi-Fi 6 and newer AP models, these limitations no longer apply due to advanced hardware capabilities, allowing for unrestricted utilisation of multicast optimisation.

Broadcast

Broadcast key rotation

What is it?

The WPA and WPA2/3 security protocols use pairwise keys for unicast packets and group keys for multicast packets. “Broadcast key rotation” specifies how often the AP generates a new group key for broadcast and multicast packets.

Why use it?

Any device in the area of a wireless access point can see the traffic transmitted by the AP. The broadcast/multicast traffic is encrypted by what is commonly known as a GTK (Group Temporal Key). By default, the key is not rotated which exposes the security of the key. Indeed, malicious equipment can guess the key and then decrypt the traffic. For this reason, it is recommended to periodically modify the GTK to overcome this risk.

How does it work?

The last question is how these new GTKs are transmitted. The new keys have to be sent to the wireless clients in a secure way. To do this, the new GTK is delivered by unicast to each of the APs clients and then encrypted with each client’s PTK.

Configuration

You can specify how often the “Group Temporal Key” will be rotated.



Broadcast/Multicast Optimization

Broadcast Key Rotation ENABLED

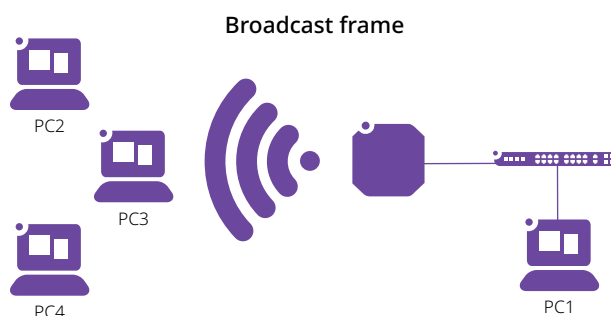
Broadcast Key Rotation Time Interval min(s) ▼ ▲

Address Resolution Protocol (ARP) filtering

What is It?

A feature called “**Filter ARP**” allows the AP to act as an “ARP Proxy”. If the ARP request packet asks for a client’s MAC address and the AP knows the client’s MAC and IP address, then the AP will answer the ARP request but will not forward the ARP request to all broadcast domains. This reduces the forwarding of ARP broadcast packets and significantly improves network performance by avoiding non-necessary traffic.

How does it work?



Let’s suppose PC1 wants to know the MAC Address of PC2. PC1 will send an “ARP Request” packet. This packet is natively broadcast as you can see below.

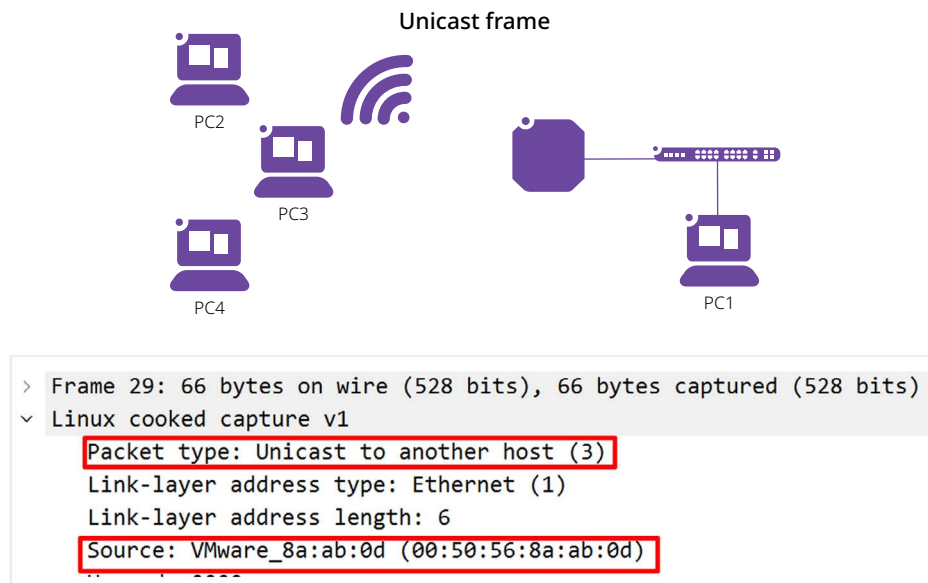
```
> Frame 14: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
v Linux cooked capture v1
  Packet type: Broadcast (1)
    Link-layer address type: Ethernet (1)
    Link-layer address length: 6
    Source: VMware_8a:ab:0d (00:50:56:8a:ab:0d)
```

If you have many devices connected to your wireless network, then many broadcast packets will be transmitted. The problem is all devices will wake up even if the traffic does not involve them. This causes unnecessary power consumption.

To overcome this issue, OmniAccess Stellar APs implement a feature that converts “broadcast” packets to “unicast”. When PC1 sends an ARP request packet, the AP will not forward this “broadcast” packet if the destination client is known by the AP. To do that the AP will check its ARP table.

```
root@AP-29:C0:~# arp
IP address      HW type        Flags          HW address     Mask           Device
172.20.1.1      0x1            0x2            00:50:56:9f:1d:33  *             br-wan
172.20.1.103    0x1            0x2            dc:08:56:13:39:a0  *             br-wan
172.20.1.102    0x1            0x2            64:bc:58:e7:84:39  *             br-wan
172.20.1.254    0x1            0x2            94:24:e1:55:8b:7d  *             br-wan
172.20.1.108    0x1            0x2            44:01:bb:88:2a:b6  *             br-wan
172.20.1.106    0x1            0x0            44:01:bb:88:2c:46  *             br-wan
172.20.1.2      0x1            0x2            00:50:56:9f:a4:2b  *             br-wan
```

If the destination client is already known by the AP, then the AP will rewrite the “ARP request” packet as unicast.



Conversion to unicast will save power to other wireless devices connected to the AP and avoid non-necessary traffic.

This feature can be enabled through OmniVista on SSID parameters.



Why use it?

This feature is highly recommended in high density environments such as schools, universities, and hospitals.

Limitations

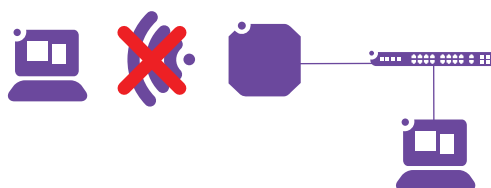
We have mentioned two types of ARP packets, ARP request and reply. But there is another type of ARP packet called gratuitous ARP. A gratuitous ARP is an ARP response that was not prompted by an ARP request. The gratuitous ARP is sent as a broadcast, as a way for a device to announce or update its IP to MAC mapping to the entire network. A gratuitous ARP packet will not have special treatment by an OmniAccess Stellar AP. “GARP” will be sent as broadcast.

All protocols filtering

What is it?

The “Broadcast Filter-All” functionality will drop any broadcast traffic, and as such, must be approached carefully. It is important to note that once this feature is activated, all broadcast frames are discarded, except for the essential DHCP and Address Resolution Protocol (ARP) frames, which are necessary for proper network communication. It is therefore crucial to understand all the potential implications of enabling this feature, and carefully evaluate the specific network requirements before enabling it.

Broadcast frame



The configuration is implemented at the SSID configuration level.

Broadcast Filter All

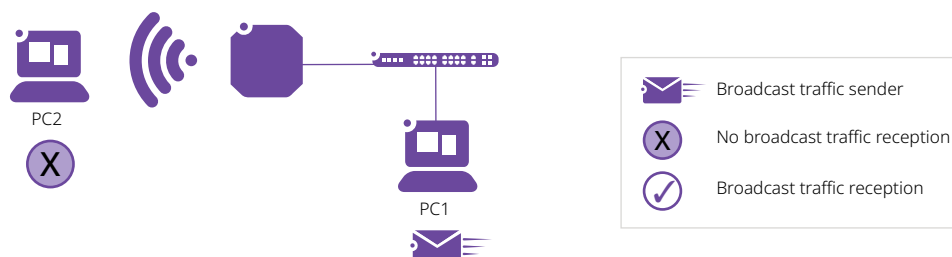
ENABLED

How does it work?

To understand in detail how this feature works, we will look at several scenarios.

Scenario 1

In this scenario we have a wired client, PC1, and a wireless client, PC2, with the intended objective of generating broadcast traffic. This demonstration showcases the APs non-forwarding of broadcast traffic to the wireless clients. To perform this test, we will use the “iperf” tool.



Name	IP Address/CIDR	VLAN
PC1	192.168.35.1/24	35
PC2	192.168.35.2/24	35

We initiate the generation of broadcast traffic from PC1 to the address 192.168.35.255, while concurrently commencing a Wireshark capture to examine the transmitted traffic.

No.	Time	Source	Destination
377	7.984548	192.168.35.1	192.168.35.255
408	8.975880	192.168.35.1	192.168.35.255
431	9.970427	192.168.35.1	192.168.35.255
465	10.953581	192.168.35.1	192.168.35.255
497	11.955882	192.168.35.1	192.168.35.255

Throughout the transmission, we also initiated a Wireshark capture on wireless client PC2.

No.	Time	Source	Destination
-----	------	--------	-------------

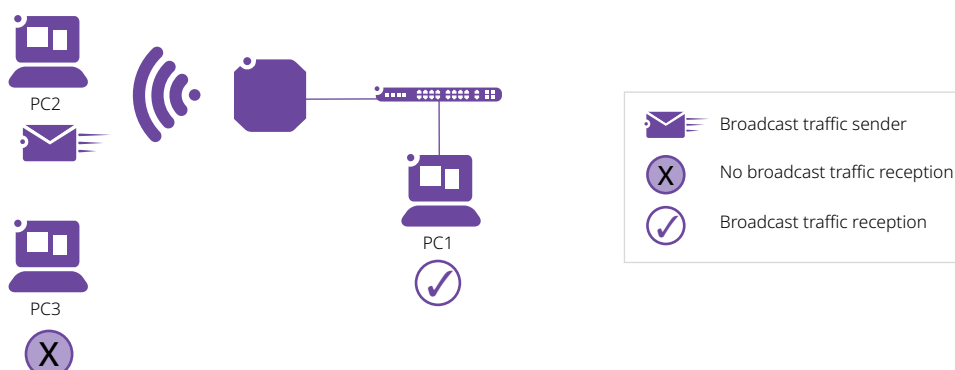
It can be easily seen that the OmniAccess Stellar AP did not forward the broadcast stream to the wireless clients, specifically PC2.

Application note

Alcatel-Lucent OmniAccess Stellar Access Point

Scenario 2

In this situation, we are going to generate broadcast traffic from a wireless device known as PC2. Then, we will investigate if this traffic is successfully received by other wireless devices connected to the same Wi-Fi network (known as SSID) as PC2. Additionally, we will also verify if wired devices (PC1) that belong to the same VLAN are able to receive this traffic.



Name	IP Address/CIDR	VLAN
PC1	192.168.35.1/24	35
PC2	192.168.35.2/24	35
PC3	192.168.35.4/24	35

On the PC2 Wireshark capture we can see the broadcast traffic generated.

No.	Time	Source	Destination
27	0.558100	192.168.35.2	192.168.35.255
225	1.542486	192.168.35.2	192.168.35.255
432	2.558092	192.168.35.2	192.168.35.255
526	3.542565	192.168.35.2	192.168.35.255

Now, let's take a look on the other wireless client (PC3). We can see that the OmniAccess Stellar AP has successfully dropped this traffic.

No.	Time	Source	Destination

Finally, we will analyse the Wireshark capture on the wired client (PC1). We can see that wired clients on the same VLAN receive the broadcast traffic. To conclude, the broadcast traffic is transmitted on the LAN through the OmniAccess Stellar AP uplink.

No.	Time	Source	Destination
4	0.064994	192.168.35.2	192.168.35.255
48	1.065062	192.168.35.2	192.168.35.255
66	2.080211	192.168.35.2	192.168.35.255
91	3.080469	192.168.35.2	192.168.35.255

Why use it?

Primarily, this functionality serves to prevent unnecessary traffic on the network. This filter can effectively extend the battery lifespan of wireless devices connected to the network such as laptops, smartphones and IoT devices. It is strongly advised to employ this attribute in areas that are densely populated with wireless devices.

Application note

Alcatel-Lucent OmniAccess Stellar Access Point

Conclusion

We have provided an overview of techniques to improve the efficiency of multicast and broadcast traffic on Wi-Fi networks. We have looked at how to filter broadcast packets to significantly improve network performance and preserve battery life on wireless devices by avoiding unnecessary traffic. And, we have seen how we can use broadcast key rotation to improve security.