

Troubleshoot Multicast on C9800 Wireless LAN Controller

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Internet Group Management Protocol Overview](#)

[Multicast Modes on WLC](#)

[Multicast Traffic Handling by WLC](#)

[Multicast Support Per Platform](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Step 1: AP Sends an IGMP Join to WLC](#)

[Step 2: Client Sends an IGMP Join for Multicast Stream](#)

[Step 3: WLC Processes the Join Request](#)

[Step 4: Multicast Traffic Delivery to WLC](#)

[Step 5: CAPWAP Multicast Forwarding to AP\(s\)](#)

[Step 6: AP Forwards the Multicast Traffic to Clients](#)

[FlexConnect Local Switching Mode](#)

[Related Information](#)

Introduction

This document describes the multicast workflow, configuration, and troubleshooting on the Cisco C9800 Wireless LAN Controller.

Prerequisites

Requirements

- Cisco recommends that you have knowledge of these topics:
- Multicast concepts
- 9800 Wireless LAN Controller(WLC) configuration

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 9800 Wireless Controller Series (Catalyst 9800-40), Cisco IOS® XE Cupertino 17.12.5
- Catalyst 3560 Series Switch, Cisco IOS® 15.2.4E10
- Access Point C9115AXE, Access Point CW9164I

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Multicast is a protocol that sends packets from a single source to a group-based destination address. Only hosts that have expressed interest in receiving the packets receive them.

Internet Group Management Protocol Overview

Internet Group Management Protocol (IGMP) is used to dynamically register individual hosts as members of a multicast group on a specific LAN.

IGMP Snooping is a process by which a switch listens to IGMP network traffic between hosts and routers to build and maintain a table of client MAC addresses that are interested in receiving specific multicast streams. By snooping on IGMP packets, the switch can manage multicast traffic efficiently and prevent unnecessary flooding. Without IGMP Snooping, multicast traffic is treated similarly to broadcast traffic, reaching all devices on the segment.

IGMP Message Types:

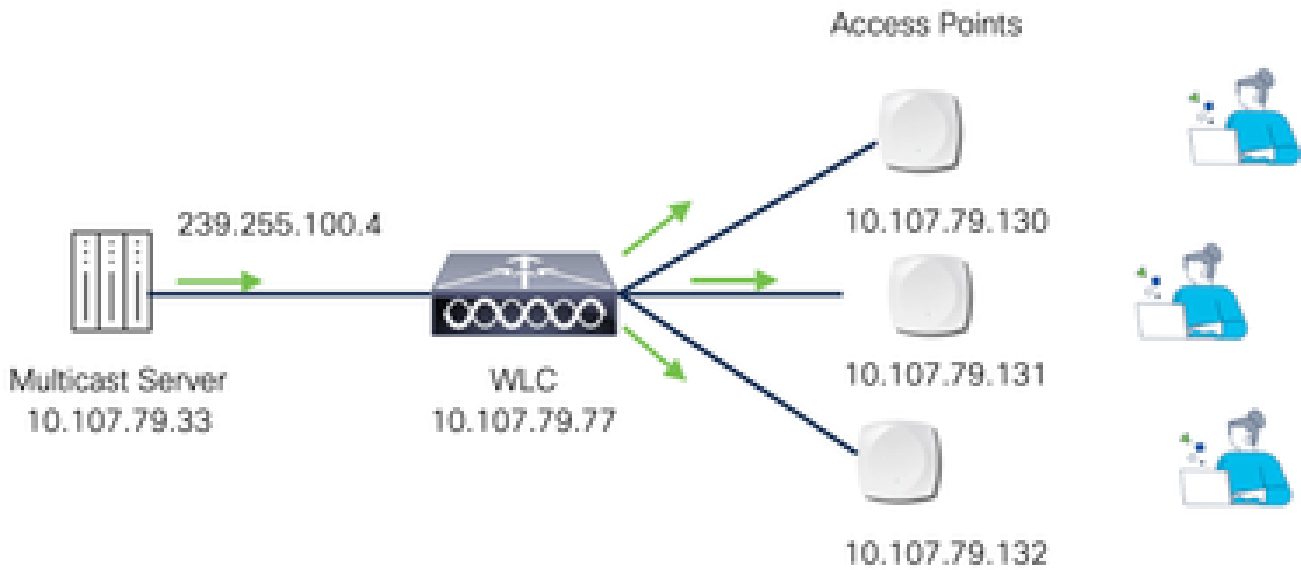
- **Membership Query:**
Sent by a router or a switch with IGMP Snooping enabled to determine if there are any interested receivers for a specific multicast group. Queries can be general, group-specific, or group-and-source-specific (the latter is used in IGMPv3)
- **Membership Report:**
Sent by a host to indicate interest in joining a multicast group or in response to a membership query. This message type is also known as an IGMP Join
- **Leave Group Message:**
Sent by a host when it no longer wishes to receive multicast traffic for a particular group.

IGMP Versions:

- **IGMPv1:** Uses a basic query-response model, allowing multicast routers and multilayer switches to determine which multicast groups have active members on a subnet. Hosts can join or leave groups as specified in RFC 1112.
- **IGMPv2:** Enhances functionality by introducing the leave process (reducing leave latency), group-specific queries, and explicit maximum query response time. It also allows routers to elect an IGMP querier independently of the multicast protocol. For more details, refer to RFC 2236.
- **IGMPv3:** Adds support for Source-Specific-Multicast (SSM), enabling hosts to specify the sources from which they want to receive multicast traffic for a group. IGMPv3 uses the multicast address 224.0.0.22 for membership reports and includes detailed "Group Records" to convey source information. For more details, refer to RFC 3376.

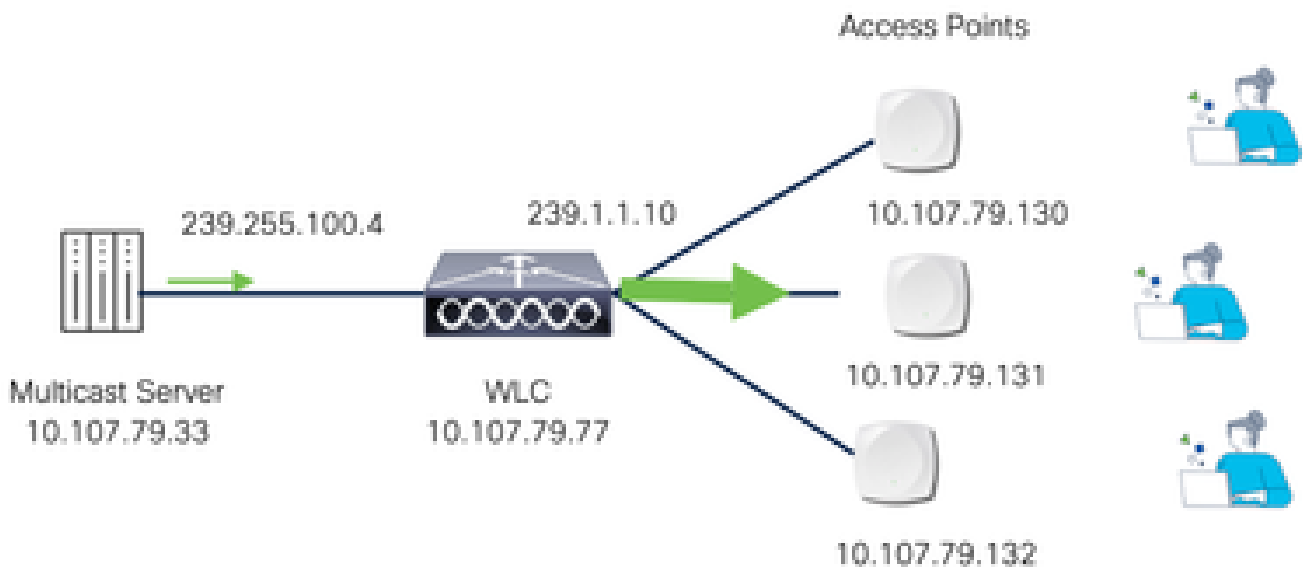
Multicast Modes on WLC

- Unicast mode: The controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient and generates a lot of extra traffic in the device and the network but is required on networks that do not support multicast routing (needed if the APs are on different subnets than the Wireless Management Interface(WMI) of the device).



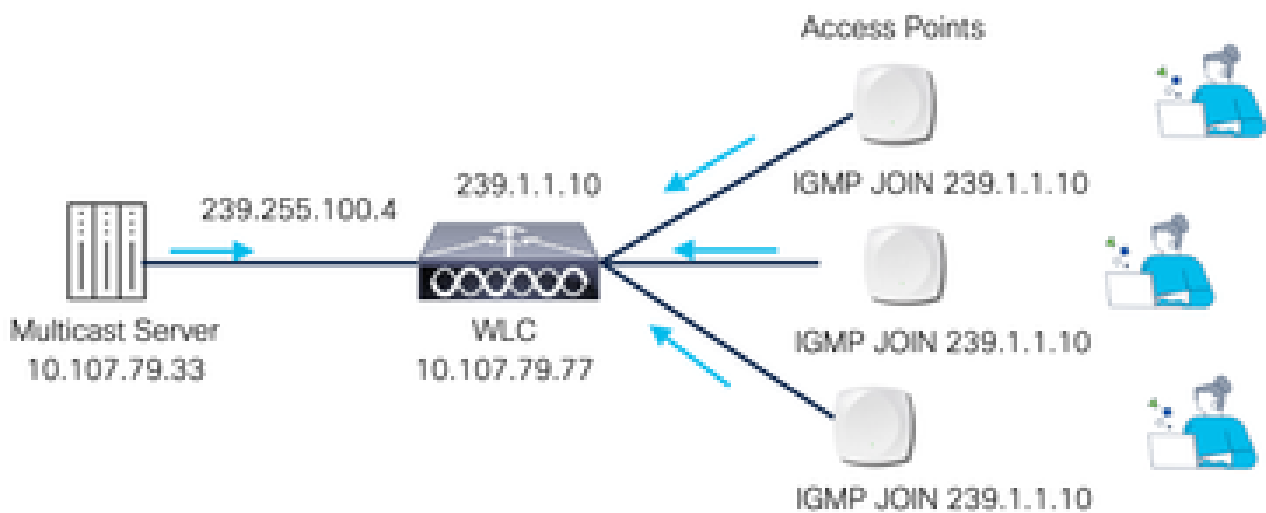
Multicast-over-Unicast

- Multicast mode: The controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the controller processor and shifts the work of packet replication to the network, which is much more efficient than the unicast method.



Multicast-over-Multicast

To receive multicast traffic, Access Points (APs) send an IGMP Join membership report to the configured Multicast CAPWAP Group address. This allows the APs to join the multicast group and start receiving the associated multicast traffic.



AP IGMP Join

Multicast Traffic Handling by WLC

A single CAPWAP multicast group address is used to deliver multicast traffic across WLANs. To manage this, the controller maintains a Layer 2 table that maps its interfaces to WLANs using unique multicast group IDs (MGIDs), identifying where multicast traffic must be sent. An MGID is a 14-bit value placed in the 16-bit reserved field of the CAPWAP header, with the remaining 2 bits set to zero.

Not all clients on a WLAN need the same multicast traffic. To identify interested clients, IGMP snooping enables access points to listen for IGMP membership reports from hosts. Based on this, the controller builds a Layer 3 multicast group table. Each entry includes the MGID, CAPWAP multicast group address, and VLAN ID. It also lists specific clients that joined the group and the APs they are associated with.

When the multicast mode is enabled and the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The controller always uses the management VLAN for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the VLAN on which clients receive multicast traffic.

Multicast Support Per Platform

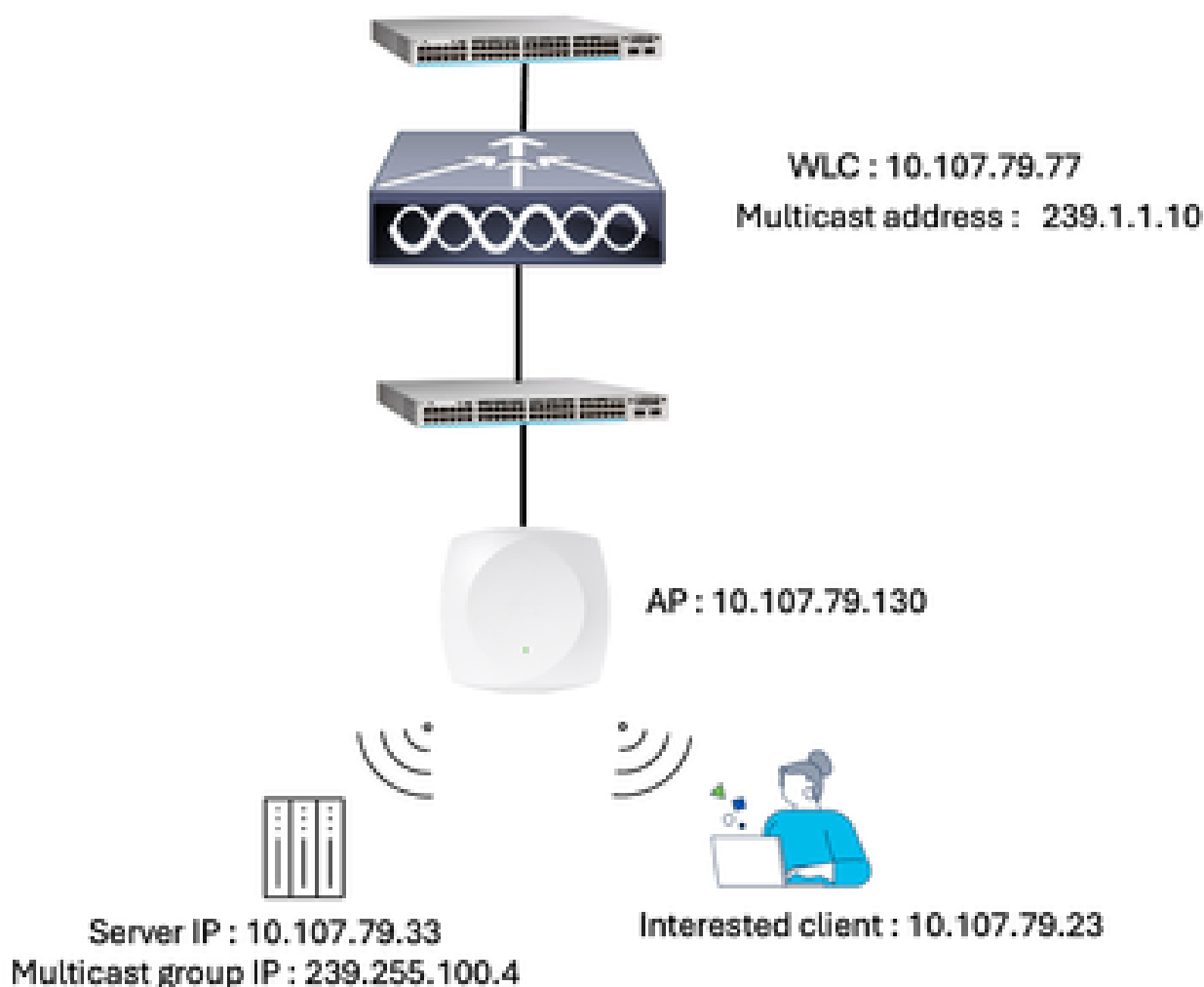
Table 1. Multicast Support Per Platform

Platform	MulticastSupport - Multicastover Unicast	MulticastSupport - MulticastoverMulticast
Cisco Catalyst 9800-40 Wireless Controller	No	Yes
Cisco Catalyst 9800-80 Wireless Controller	No	Yes
Cisco Catalyst 9800 Wireless Controller	Yes	Yes

Platform	MulticastSupport - Multicastover Unicast	MulticastSupport - MulticastoverMulticast
for Cloud- Small Template		
Cisco Catalyst 9800 Wireless Controller for Cloud- Medium Template	No	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud- Large Template	No	Yes
Cisco Catalyst 9800-L Wireless Controller	Yes	Yes

Configure

Network Diagram



Configurations

To configure multicast from the WLC GUI, go to **Configuration > Services > Multicast**. Enable **Global Wireless Multicast Mode**, select **AP CAPWAP Multicast** as **Multicast**, enter the CAPWAP multicast group address, and click **Apply**. Use an address from the 239.0.0.0/8 subnet and ensure it is unique within the network.

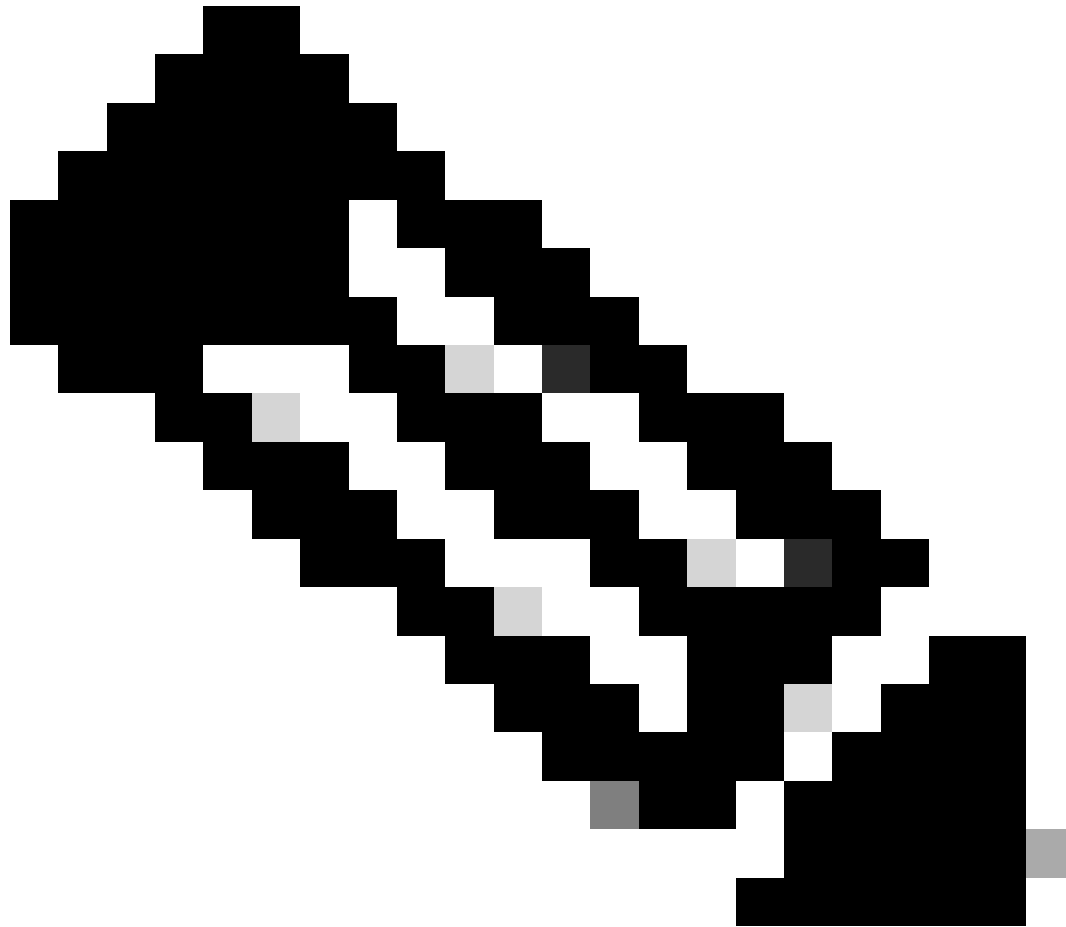
Configuration > Services > Multicast

Global Wireless Multicast Mode	ENABLED <input checked="" type="checkbox"/>
AP CAPWAP Multicast	Multicast ▼
AP CAPWAP IPv4 Multicast group Address	239.1.1.10
AP CAPWAP IPv6 Multicast group Address	::
Wireless mDNS Bridging	<input type="checkbox"/> DISABLED
Wireless Non-IP Multicast	<input type="checkbox"/> DISABLED
Wireless Broadcast	<input type="checkbox"/> DISABLED
IGMP Snooping Querier	<input type="checkbox"/> DISABLED
IGMP Snooping	ENABLED <input checked="" type="checkbox"/>
Last Member Querier Interval (milliseconds)	1000

Multicast GUI Configuration

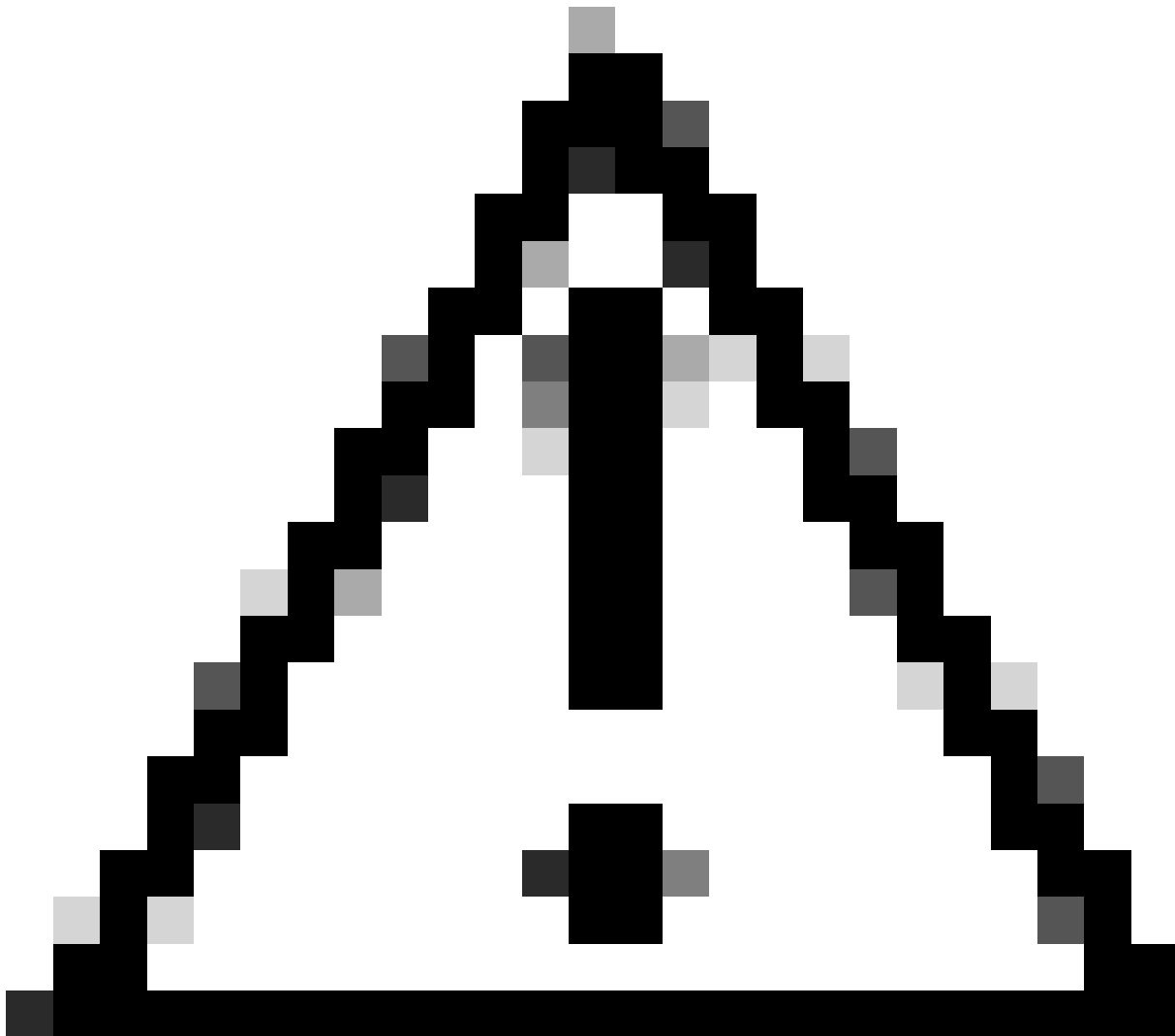
WLC CLI

```
WLC#conf t
WLC(config)#wireless multicast 239.1.1.10
```



Note: When the AP and WLC are in the same VLAN, enable IGMP snooping on all intermediate switches.

For deployments where the AP and WLC are in different VLANs, enable IP multicast routing globally, configure PIM (Protocol Independent Multicast) on the relevant router interfaces, and enable IGMP on the switches.



Caution: You must be cautious when using IGMPv3 with switches that are enabled for IGMP snooping. The IGMPv3 messages are different from the messages used in IGMP Version 1 (IGMPv1) and Version 2 (IGMPv2). If your switch does not recognize IGMPv3 messages, the hosts do not receive traffic when IGMPv3 is used.

IGMPv3 devices do not receive multicast traffic in either cases: When IGMP snooping is disabled. When IGMPv2 is configured on the interface. It is recommended to enable IGMPv3 on all intermediate or other Layer 3 network devices. Primarily, on each subnet used by multicast devices including controller and AP subnets.

Verify

Use the command to verify multicast configuration on the WLC.

```
WLC#show wireless multicast
```

```
Multicast                : Enabled
```

```
AP Capwap Multicast      : Multicast
```


AP Capwap IPv4 Multicast group Address : 239.1.1.10

AP Capwap IPv6 Multicast group Address : ::

Wireless Broadcast : Disabled

Wireless Multicast non-ip-mcast : Disabled

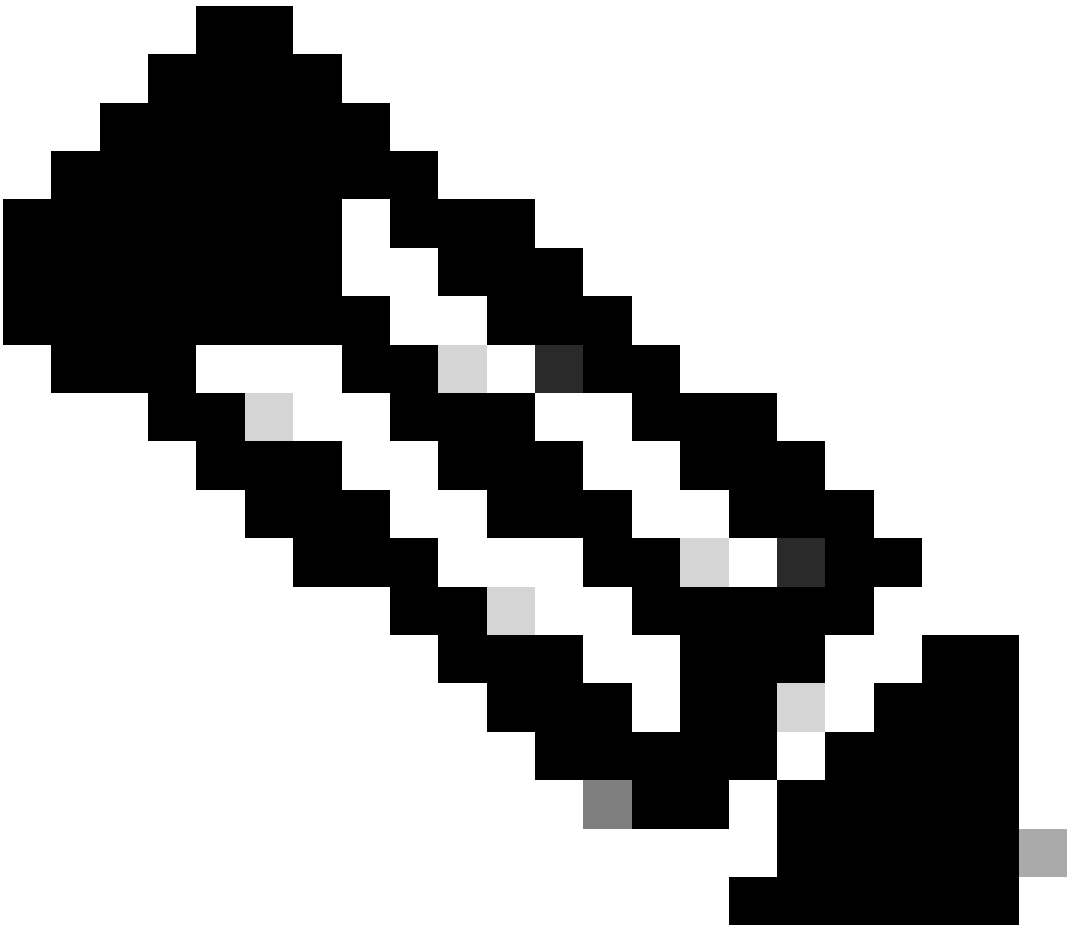
Wireless Multicast link-local : Disabled

Check the AP and WLC connection for multicast traffic using this command.

WLC#show ap multicast mom

AP Name	MOM-IP TYPE	MOM-STATUS

AP2	IPv4	Up
AP7	IPv4	Up



Note: The MOM-STATUS displays as "UNKNOWN" for certain Cisco IOS Access Point models. This occurs because these APs do not send the MoM payload to the controller. The affected models include: Cisco Aironet 1702i Access Point, Cisco Aironet 3702i/3702e Access Point, Cisco IW3702 Access Point. For more details, refer [CSCwd12261](#).

Use this command to view MGID and associated VLANs (Layer 2 table).

```
WLC#sh ip igmp snooping wireless mgid
```

```
Total number of L2-MGIDs   = 1
```

```
Total number of MCAST MGIDs = 2
```

Wireless multicast is Enabled in the system:

```
Vlan bcast   nonip-mcast mcast   mDNS-br  mgid   mcast-link-local Stdbby Flags
```

1	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	0:1:1:0
100	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	0:1:1:0
1002	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	0:1:1:0
1003	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	0:1:1:0
1004	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	0:1:1:0
1005	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	0:1:1:0
1415	Disabled	Disabled	Enabled	Enabled	Enabled	Disabled	0:1:1:1

```
Index MGID   (S, G, V)
```

```
-----  
386  4160   (0.0.0.0, 239.255.255.250, 1415)
```

```
636  4161   (0.0.0.0, 239.255.100.4, 1415)
```

```
WLC#sh ip igmp snooping groups vlan 1415
```

```
Vlan   Group           Type      Version  Port List
```

```
-----  
1415  239.255.100.4      igmp      v2       Ca2  
1415  239.255.255.250    igmp      v2       Ca2
```

Run this command to check client membership information (Layer 3 table).

```
WLC#sh wireless multicast source 0.0.0.0 group 239.255.100.4 vlan 1415
```

```
Group : 239.255.100.4
```

Vlan : 1415

MGID : 4161

Client List

Client MAC	Client IP	Status
------------	-----------	--------

242f.d0da.a7da	10.107.79.23	MC_ONLY
-----------------------	---------------------	----------------

WLC#sh ip igmp snooping igmpv2-tracking

Client to SGV mappings

Client: 10.107.79.23 Port: Ca2

Group: 239.255.255.250 Vlan: 1415 Source: 0.0.0.0 Blocklist: no

Group: 239.255.100.4 Vlan: 1415 Source: 0.0.0.0 Blocklist: no

Client: 10.107.79.33 Port: Ca2

Group: 239.255.255.250 Vlan: 1415 Source: 0.0.0.0 Blocklist: no

SGV to Client mappings

Group: 239.255.100.4 Source: 0.0.0.0 Vlan: 1415

Client: 10.107.79.23 Port: Ca2 Blocklist: no

Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 1415

Client: 10.107.79.33 Port: Ca2 Blocklist: no

Client: 10.107.79.23 Port: Ca2 Blocklist: no

Use the command to verify multicast configuration on the AP.

AP2#sh capwap mcast mgid clients

Client for each MGID:

mgid	type	client slot vap
------	------	-----------------

4160	mc_only	24:2F:D0:DA:97:51 1 0
------	---------	-----------------------

4160	mc_only	24:2F:D0:DA:A7:DA 0 0
------	---------	-----------------------

4161 mc_only 24:2F:D0:DA:A7:DA 0 0

9606 mc2uc 24:2F:D0:DA:97:51 1 0

9606 mc2uc 24:2F:D0:DA:A7:DA 0 0

MGID for each Client:

client	ip	port	mgid
--------	----	------	------

24:2F:D0:DA:97:51	10.107.79.33	apr1v0	4160
-------------------	--------------	--------	------

24:2F:D0:DA:A7:DA	10.107.79.23	apr0v0	4160
-------------------	--------------	--------	------

4161

AP2#sh capwap mcast mgid all

mgid	wlan_bit_map_all	mc2uc_cli	mc_only_cl	type	rx_pak_cnt	tx_pak_slot0	tx_pak_slot1	tx_pak_slot2	tx_pak_slot3	tx_pak_rlan
------	------------------	-----------	------------	------	------------	--------------	--------------	--------------	--------------	-------------

1415	00000000000000000001	0	0	0	36367	12189	1199758	634	0	0
------	----------------------	---	---	---	-------	-------	---------	-----	---	---

4097	11111111111111111111	0	0	0	0	0	0	0	0	0
------	----------------------	---	---	---	---	---	---	---	---	---

4160	00000000000000000001	0	1	1	36	36	36	0	0	0
------	----------------------	---	---	---	----	----	----	---	---	---

4161	00000000000000000001	0	1	1	10091	10091	0	0	0	0
------	----------------------	---	---	---	-------	-------	---	---	---	---

9606	00000000000000000000	1	0	3	160	154	2	0	0	0
------	----------------------	---	---	---	-----	-----	---	---	---	---

Troubleshoot

Collect embedded packet capture (EPC) from the WLC to understand the traffic flow. Refer to the link for the steps to collect EPC. [Troubleshoot Catalyst 9800 Wireless LAN Controllers.](#)

This is a list of the source, destination, and other relevant IP addresses observed in the annotated Wireshark captures. These correspond to the key packet flows shown in the figures, helping to identify which hosts initiated and received each packet.

WLC WMI - 10.107.79.77

AP IP - 10.107.79.130

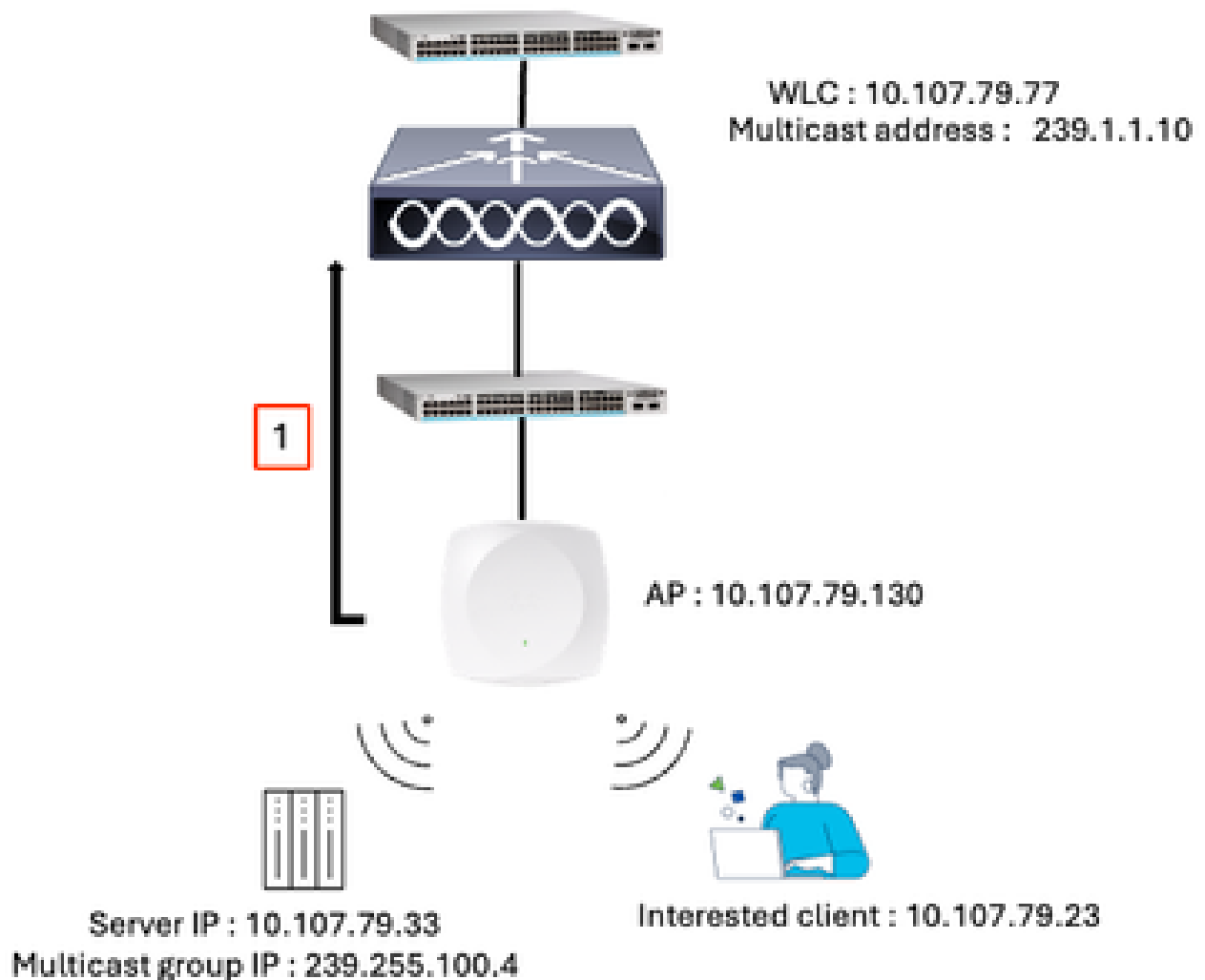
CAPWAP Multicast group IP address configured on WLC - 239.1.1.10

Multicast source endpoint IP - 10.107.79.33

Multicast traffic IP - 239.255.100.4

Client IP (Destination) - 10.107.79.23

Step 1: AP Sends an IGMP Join to WLC



AP IGMP Join

The AP joins the CAPWAP multicast group (239.1.1.10) of the controller, using IGMP.

No.	Time	Delta	Source	Destination	Protocol	Info
23472	2025-08-1...	0.0...	10.107.79.33	224.0.0.252	IGMPv2	Membership Report group 224.0.0.252
23488	2025-08-1...	0.2...	10.107.79.23	224.0.0.251	IGMPv2	Membership Report group 224.0.0.251
24387	2025-08-1...	0.8...	10.107.79.130	239.1.1.10	IGMPv2	Membership Report group 239.1.1.10
24470	2025-08-1...	0.0...	10.107.79.119	224.0.0.252	IGMPv2	Membership Report group 224.0.0.252
24471	2025-08-1...	0.0...	10.107.79.119	224.0.0.252	IGMPv2	Membership Report group 224.0.0.252
24472	2025-08-1...	0.0...	10.107.79.119	224.0.0.252	IGMPv2	Membership Report group 224.0.0.252

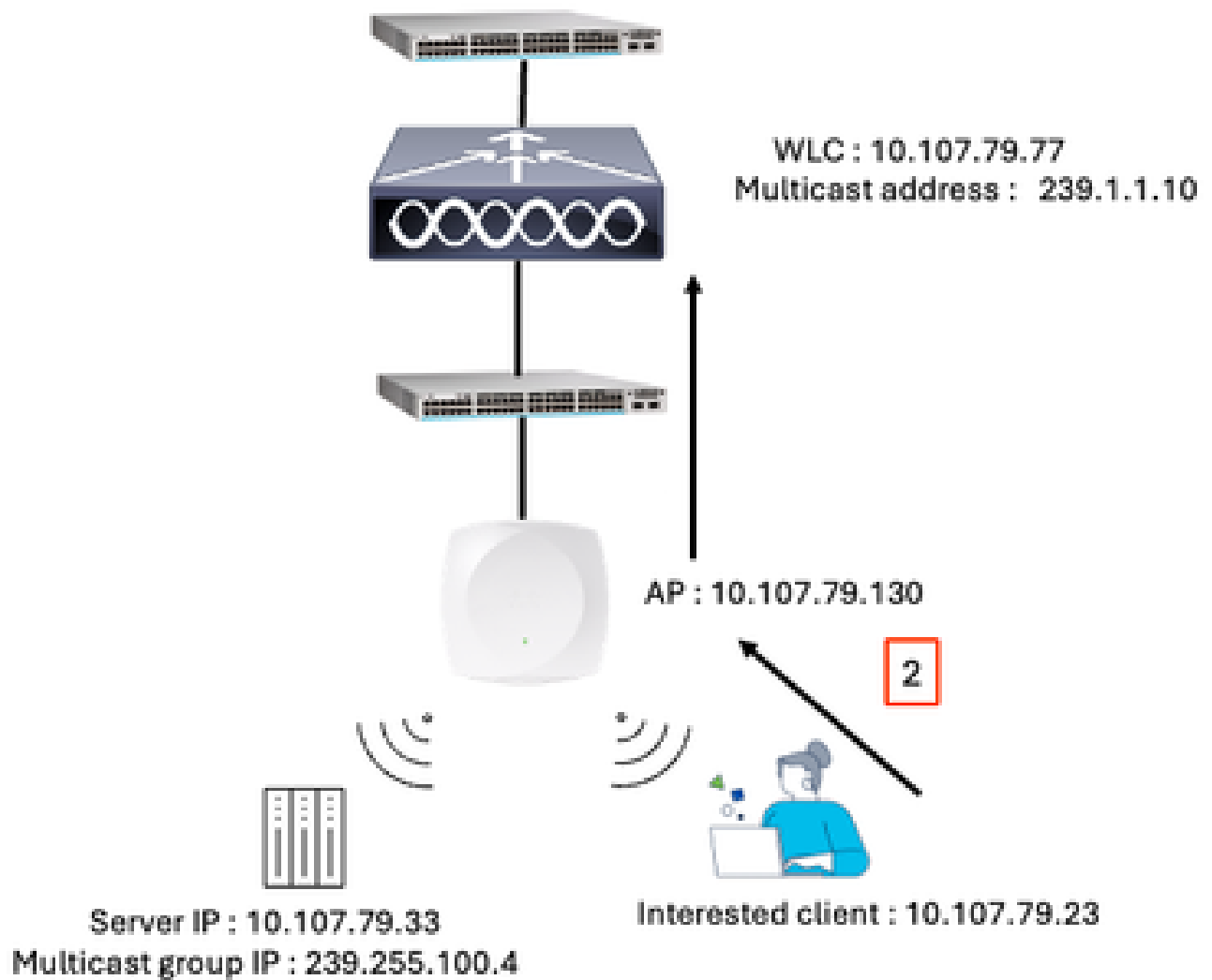
> Frame 24387: 50 bytes on wire (400 bits), 50 bytes captured (400 bits)		Ethernet
> Ethernet II, Src: CiscoMeraki_f5:68:e0 (cc:9c:3e:f5:68:e0), Dst: IPv4mcast_01:01:0a (01:00:5e:01:01:0a)		0
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415		
> Internet Protocol Version 4, Src: 10.107.79.130, Dst: 239.1.1.10		
Internet Group Management Protocol		
[IGMP Version: 2] Type: Membership Report (0x16) Max Resp Time: 0.0 sec (0x00) Checksum: 0xf9f3 [correct] [Checksum Status: Good] Multicast Address: 239.1.1.10		

Internet Group Management Protocol (igmp), 8 bytes

Packets: 189081 · Displayed: 253 (0.1%)

Profile: My preferences

Step 2: Client Sends an IGMP Join for Multicast Stream



Client IGMP join for multicast stream

The wireless client sends an IGMP join request to indicate interest in a specific multicast group.

The associated Access Point (AP) encapsulates the client IGMP Join request within a CAPWAP tunnel and sends it as unicast traffic to the Wireless LAN Controller (WLC).

Example:

A client sends an IGMP Membership Report for multicast group address 239.255.100.4.

No.	Time	Delta	Source	Destination	Protocol	Info
11	2025-08...	0.0000...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4
17	2025-08...	0.0902...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4
526	2025-08...	4.3632...	0.0.0.0	224.0.0.1	IGMPv2	Membership Query, general
544	2025-08...	0.1461...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4
625	2025-08...	0.4933...	10.107.79.23	224.0.0.251	IGMPv2	Membership Report group 224.0.0.251
830	2025-08...	1.5094...	10.107.79.23	239.255.255.250	IGMPv2	Membership Report group 239.255.255.250
889	2025-08...	0.2901...	10.107.79.77	224.0.0.1	IGMPv2	Membership Query, general
918	2025-08...	0.2094...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4
> Frame 11: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{F7DB08DB...} Ethernet > Ethernet II, Src: TPLink_da:a7:da (24:2f:d0:da:a7:da), Dst: IPv4mcast_7f:64:04 (01:00:5e:7f:64:04) > Internet Protocol Version 4, Src: 10.107.79.23, Dst: 239.255.100.4 > Internet Group Management Protocol [IGMP Version: 2] Type: Membership Report (0x16) Max Resp Time: 0.0 sec (0x00) Checksum: 0x95fb [correct] [Checksum Status: Good] Multicast Address: 239.255.100.4						

Client sends IGMP membership report for the interested Multicast traffic - Captures collected from endpoint

The AP (IP: 10.107.79.130) encapsulates this request in a CAPWAP tunnel and sends it to the WLC (IP: 10.107.79.77).

No.	Time	De	Source	Destination	Protocol	Info
52506	2025-08...	...	10.107.79.23	239.255.255.250	IGMPv2	Membership Report group 239.255.255.250
53999	2025-08...	...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4
54289	2025-08...	...	10.107.79.33	224.0.0.251	IGMPv2	Membership Report group 224.0.0.251
54291	2025-08...	...	10.107.79.33	224.0.0.251	IGMPv2	Membership Report group 224.0.0.251
54292	2025-08...	...	10.107.79.33	224.0.0.251	IGMPv2	Membership Report group 224.0.0.251
54294	2025-08...	...	10.107.79.33	224.0.0.251	IGMPv2	Membership Report group 224.0.0.251
> Frame 53999: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) > Ethernet II, Src: CiscoMeraki_f5:68:e0 (cc:9c:3e:f5:68:e0), Dst: Cisco_c9:78:6b (90:eb:50:c9:78:6b) > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415 > Internet Protocol Version 4, Src: 10.107.79.130, Dst: 10.107.79.77 > User Datagram Protocol, Src Port: 5272, Dst Port: 5247 > Control And Provisioning of Wireless Access Points - Data > IEEE 802.11 QoS Data, Flags:T > Logical-Link Control > Internet Protocol Version 4, Src: 10.107.79.23, Dst: 239.255.100.4 > Internet Group Management Protocol [IGMP Version: 2] Type: Membership Report (0x16) Max Resp Time: 0.0 sec (0x00) Checksum: 0x95fb [correct] [Checksum Status: Good] Multicast Address: 239.255.100.4						

Client IGMP membership report reaches the WLC inside a CAPWAP tunnel - Captures collected from WLC

No.	Time	Delta	Source	Destination	Protocol	Info	
11373	2025...	0.0...	10.107.79.23	224.0.0.2	IGMPv2	Leave Group 239.255.100.4	
25420	2025...	15....	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4	
25515	2025...	0.2...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4	
27030	2025...	2.3...	0.0.0.0	224.0.0.1	IGMPv2	Membership Query, general	
27324	2025...	0.6...	10.107.79.23	239.255.255.250	IGMPv2	Membership Report group 239.255.255.250	
27328	2025...	0.0...	10.107.79.23	239.255.100.4	IGMPv2	Membership Report group 239.255.100.4	
28799	2025...	1.9...	10.107.79.23	224.0.0.252	IGMPv2	Membership Report group 224.0.0.252	
30117	2025...	1.7...	10.107.79.33	224.0.0.252	IGMPv2	Membership Report group 224.0.0.252	

> Frame 25420: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{4...} Ethernet II, Src: Cisco_23:a6:27 (88:9c:ad:23:a6:27), Dst: Intel_e2:83:ca (a0:36:9f:e2:83:ca)

> Internet Protocol Version 4, Src: 10.107.79.77, Dst: 10.107.79.99

> User Datagram Protocol, Src Port: 5555, Dst Port: 5000

> AiroPeek/OmniPeek encapsulated IEEE 802.11

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:TC

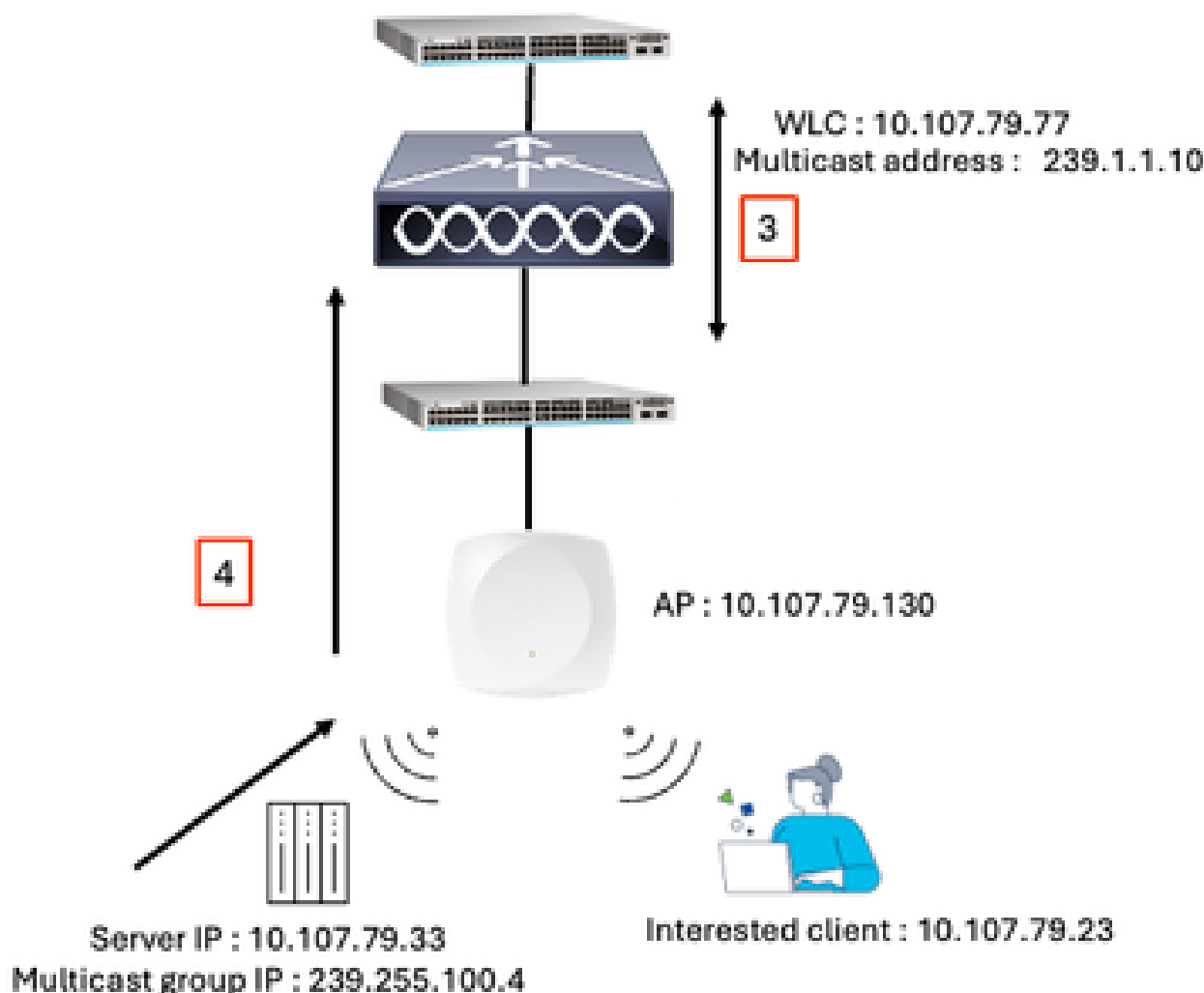
> Logical-Link Control

> Internet Protocol Version 4, Src: 10.107.79.23, Dst: 239.255.100.4

> Internet Group Management Protocol

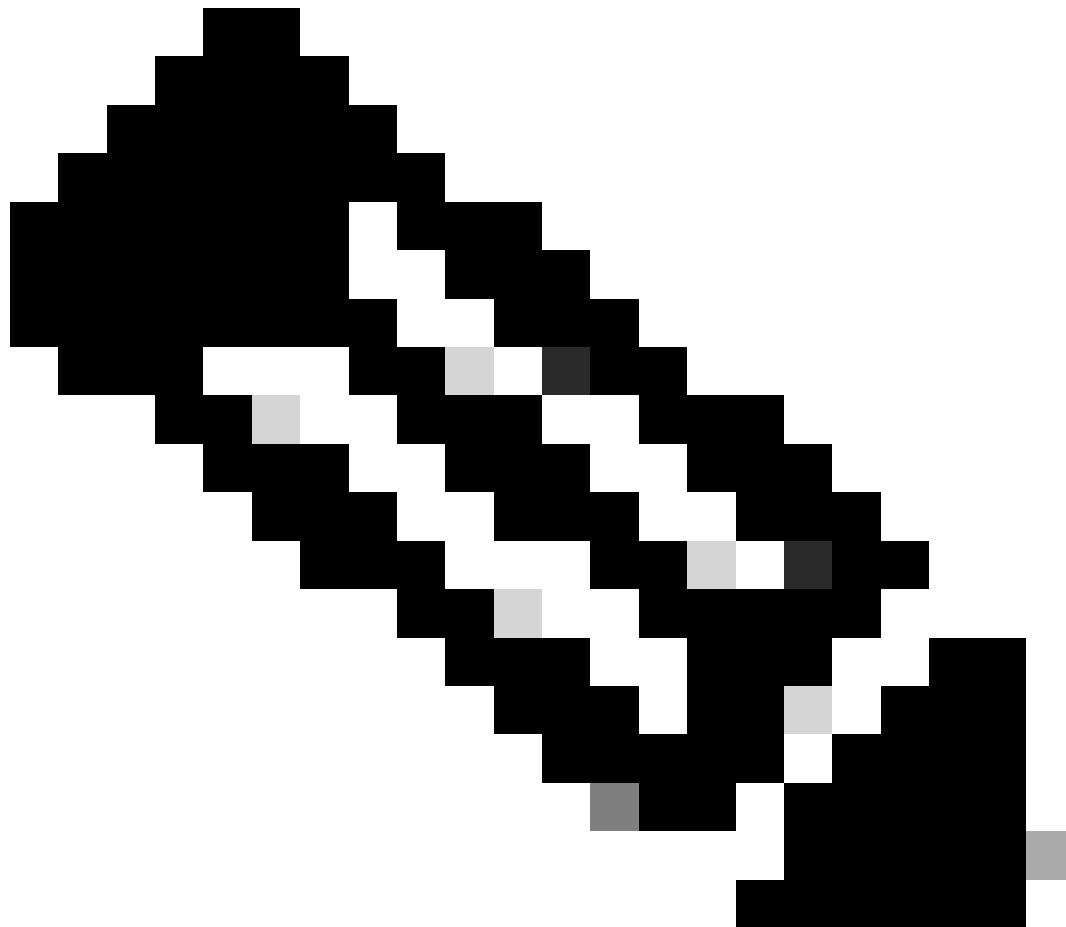
Client IGMP Join - OTA Captures

Step 3: WLC Processes the Join Request



Step 3 and 4

The WLC receives the IGMP Join, records the multicast group address, and sends an IGMP Join or relevant multicast request upstream to its connected switch or router.



Note: In this scenario, the wireless client is also acting as a multicast source.

Step 4: Multicast Traffic Delivery to WLC

The upstream switch or router forwards multicast traffic for the requested group to the WLC.

Example:

The multicast source (10.107.79.33), which is a wireless client, sends multicast traffic to group address 239.255.100.4. Because the source is wireless, the multicast traffic is encapsulated in a CAPWAP tunnel and delivered to the WLC.

No.	Time	Delta	Source	Destination	Protocol	Info
1	2025-...	0.000...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
2	2025-...	0.007...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
3	2025-...	0.008...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
4	2025-...	0.009...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
5	2025-...	0.007...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
6	2025-...	0.008...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
7	2025-...	0.007...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
8	2025-...	0.008...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
9	2025-...	0.007...	10.107.79.33	239.255.100.4	MPEG TS	video-stream
10	2025-...	0.007...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]

> Frame 9: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface \Device\NPF_{7...} Ethernet
 > Ethernet II, Src: TPLink_da:97:51 (24:2f:d0:da:97:51), Dst: IPv4mcast_7f:64:04 (01:00:5e:7f:64:04)
 > Internet Protocol Version 4, Src: 10.107.79.33, Dst: 239.255.100.4
 > User Datagram Protocol, Src Port: 55111, Dst Port: 5004
 > Real-Time Transport Protocol
 > ISO/IEC 13818-1 PID=0x64 CC=14
 > [Reassembled in: 9]
 > ISO/IEC 13818-1 PID=0x64 CC=15
 > [8 Message fragments (1457 bytes): #7(184), #7(184), #8(176), #8(184), #8(184), #8(184), #9(184), #9(184)]
 > MPEG TS Packet (reassembled)
 > Packetized Elementary Stream
 > PES extension

Multicast traffic from the source device

No.	Time	De	Source	Destination	Protocol	Info
171890	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
171893	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
171894	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...
171898	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
171907	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02...

> Frame 171893: 1452 bytes on wire (11616 bits), 1452 bytes captured (11616 bits) on interface Ethernet
 > Ethernet II, Src: CiscoMeraki_f5:68:e0 (cc:9c:3e:f5:68:e0), Dst: Cisco_c9:78:6b (90:eb:50:c9:78:6b)
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
 > Internet Protocol Version 4, Src: 10.107.79.130, Dst: 10.107.79.77
 > User Datagram Protocol, Src Port: 5272, Dst Port: 5247
 > Control And Provisioning of Wireless Access Points - Data
 > IEEE 802.11 QoS Data, Flags:T
 > Logical-Link Control
 > Internet Protocol Version 4, Src: 10.107.79.33, Dst: 239.255.100.4
 > User Datagram Protocol, Src Port: 55111, Dst Port: 5004
 > Real-Time Transport Protocol
 > ISO/IEC 13818-1 PID=0x20 CC=4
 > MPEG2 Program Map Table
 > ISO/IEC 13818-1 PID=0x11 CC=4
 > DVB Service Description Table
 > ISO/IEC 13818-1 PID=0x64 CC=0 skips=12
 > [5 Message fragments (728 bytes): #171890(176), #171890(184), #171890(184), #171890(184), #171893(0)]

Multicast traffic received from the source inside a CAPWAP Tunnel - Captures collected on WLC

No.	Time	Delta	Source	Destination	Protocol	Info
7	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02517BE, Se
9	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02517BE, Se
12	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02517BE, Se
14	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG	[MP2T fragment of a reassembled packet]
17	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	PT=MPEG-II transport streams, SSRC=0xC02517BE, Se
19	2025...	0.0...	10.107.79.33	239.255.100.4	H.264	[MP2T fragment of a reassembled packet] Program A
22	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]

> Frame 12: 1491 bytes on wire (11928 bits), 1491 bytes captured (11928 bits) on interface \Device\NPF_{...} Ethernet II, Src: Cisco_23:a6:27 (88:9c:ad:23:a6:27), Dst: Intel_e2:83:ca (a0:36:9f:e2:83:ca)

> Ethernet II, Src: Cisco_23:a6:27 (88:9c:ad:23:a6:27), Dst: Intel_e2:83:ca (a0:36:9f:e2:83:ca)

> Internet Protocol Version 4, Src: 10.107.79.77, Dst: 10.107.79.99

> User Datagram Protocol, Src Port: 5555, Dst Port: 5000

> AiroPeek/OmniPeek encapsulated IEEE 802.11

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:TC

> Logical-Link Control

> Internet Protocol Version 4, Src: 10.107.79.33, Dst: 239.255.100.4

> User Datagram Protocol, Src Port: 55111, Dst Port: 5004

> Real-Time Transport Protocol

> ISO/IEC 13818-1 PID=0x64 CC=13

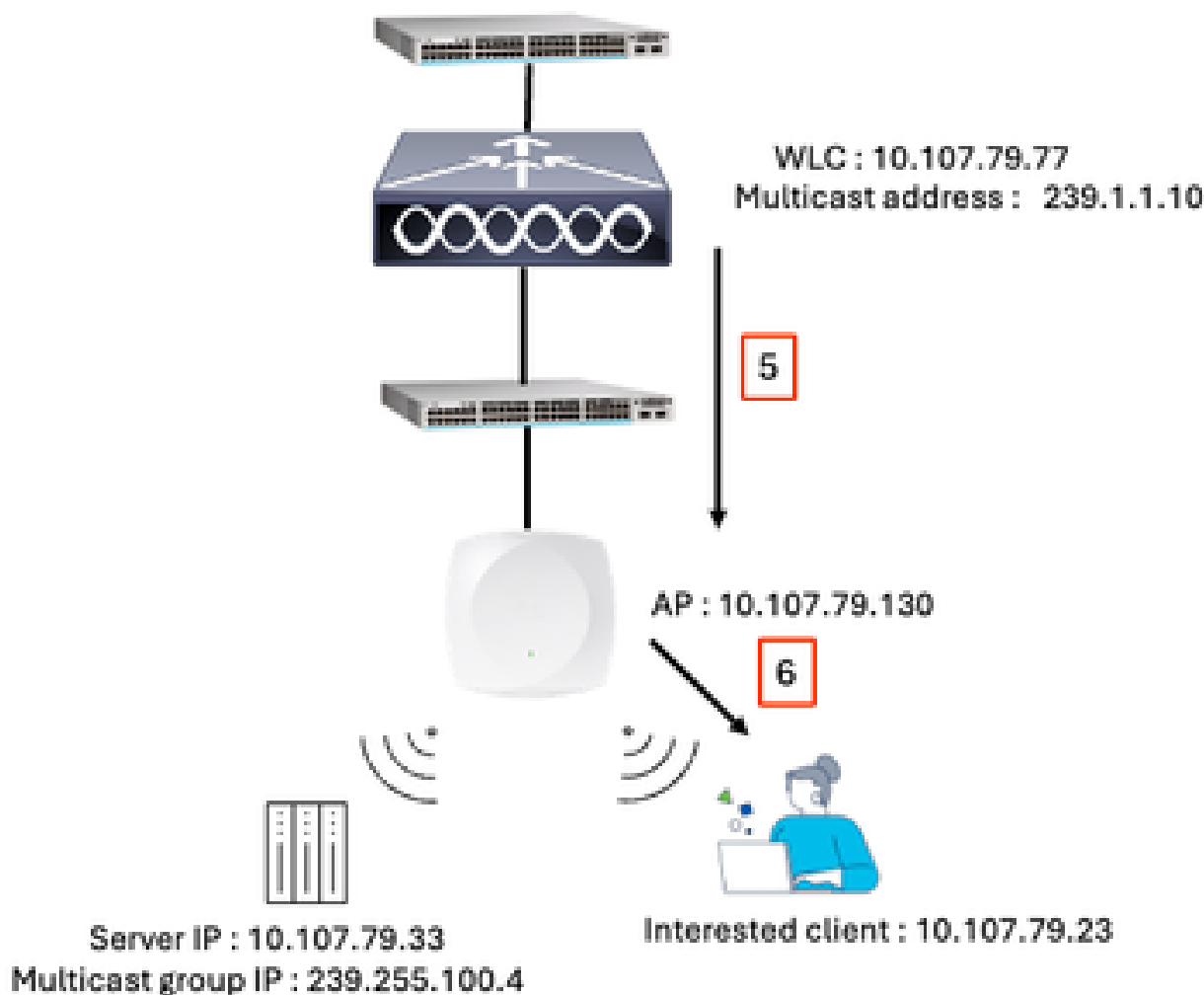
> ISO/IEC 13818-1 PID=0x64 CC=14

> ISO/IEC 13818-1 PID=0x64 CC=15

> ISO/IEC 13818-1 PID=0x64 CC=0

Multicast traffic from the source - OTA

Step 5: CAPWAP Multicast Forwarding to AP(s)



Step 5 and 6

The WLC encapsulates the multicast packets and sends them to all relevant APs using the configured

Multicast CAPWAP Group address.

Example:

The WLC forwards multicast traffic to the CAPWAP multicast group address 239.1.1.10. APs that have joined this group via IGMP (Step 1) receive the multicast stream.

No.	Time	De	Source	Destination	Protocol	Info
172594	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
172614	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	video-stream [MP2T fragment of a reasse
172640	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
172700	2025-08...	...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
172732	2025-08...	...	10.107.79.33	239.255.100.4	MPEG	video-stream [Malformed Packet: length c

> Frame 172614: 1448 bytes on wire (11584 bits), 1448 bytes captured (11584 bits)

> Ethernet II, Src: Cisco_c9:78:6b (90:eb:50:c9:78:6b), Dst: IPv4mcast_01:01:0a (01:00:5e:01:01:0a)

> Internet Protocol Version 4, Src: 10.107.79.77, Dst: 239.1.1.10

> User Datagram Protocol, Src Port: 5247, Dst Port: 5247

> Control And Provisioning of Wireless Access Points - Data

> IEEE 802.11 QoS Data, Flags:F.

> Logical-Link Control

> Internet Protocol Version 4, Src: 10.107.79.33, Dst: 239.255.100.4

> User Datagram Protocol, Src Port: 55111, Dst Port: 5004

> Real-Time Transport Protocol

> ISO/IEC 13818-1 PID=0xc8 CC=14 skips=11

> [Reassembled in: 172614]

> ISO/IEC 13818-1 PID=0x64 CC=8 skips=14

> [2 Message fragments (226 bytes): #172613(184), #172614(42)]

> MPEG TS Packet (reassembled)

> Packetized Elementary Stream

> PES extension

WLC Forwards the traffic to CAPWAP Multicast Group Address

Step 6: AP Forwards the Multicast Traffic to Clients

Each AP decapsulates the multicast packets and forwards them only to the wireless clients that have joined the multicast group.

APs use IGMP snooping to identify interested clients and ensure multicast traffic is delivered only to those clients.

	Time	Delta	Source	Destination	Protocol	Info
18	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	[MP2T fragment of a reassembled packet]
19	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	video-stream [MP2T fragment of a reassembled
20	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	[MP2T fragment of a reassembled packet]
21	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	PT=MPEG-II transport streams, SSRC=0xC02517BE, :
22	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	[MP2T fragment of a reassembled packet]
23	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	video-stream
24	2025-08...	0.0...	10.107.79.33	239.255.100.4	MPEG ...	[MP2T fragment of a reassembled packet] [MP2T f

> Frame 19: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface \Device\NPF_{...}

> Ethernet II, Src: TPLink_da:97:51 (24:2f:d0:da:97:51), Dst: IPv4mcast_7f:64:04 (01:00:5e:7f:64:04)

> Internet Protocol Version 4, Src: 10.107.79.33, Dst: 239.255.100.4

> User Datagram Protocol, Src Port: 55111, Dst Port: 5004

> Real-Time Transport Protocol

> ISO/IEC 13818-1 PID=0x64 CC=2

> [[...] 37 Message fragments (6765 bytes): #12(176), #12(184), #12(184), #12(184), #12(184), #13(184), #1

> MPEG TS Packet (reassembled)

> Packetized Elementary Stream

> PES extension

> PES header data: 3102f9a99d1102f91cfd

> PES data [...]: 0000000109f000000001419a539a8205b5b2653000208ffffea9a028b16abd0eef0e0c34ba73822de000af

> ISO/IEC 13818-1 PID=0x64 CC=3

Client receives the multicast traffic - Captures collected from the interested endpoint 10.107.79.23

No.	Time	Delta	Source	Destination	Protocol	Info
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	video-stream [Malformed Packet: length of container exceeds 65535 bytes]
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]
5...	2025...	0.0...	10.107.79.33	239.255.100.4	MPEG TS	[MP2T fragment of a reassembled packet]

> Frame 5835: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NPF{...} Ethernet II, Src: Cisco_23:a6:27 (88:9c:ad:23:a6:27), Dst: Intel_e2:83:ca (a0:36:9f:e2:83:ca)

> Internet Protocol Version 4, Src: 10.107.79.77, Dst: 10.107.79.99

> User Datagram Protocol, Src Port: 5555, Dst Port: 5000

> AiroPeek/OmniPeek encapsulated IEEE 802.11

> 802.11 radio information

> IEEE 802.11 Data, Flags:F.C

> Logical-Link Control

> Internet Protocol Version 4, Src: 10.107.79.33, Dst: 239.255.100.4

> User Datagram Protocol, Src Port: 55111, Dst Port: 5004

> Real-Time Transport Protocol

> ISO/IEC 13818-1 PID=0x64 CC=3 skips=11
[Reassembled in: 5835]

> ISO/IEC 13818-1 PID=0x64 CC=4
[Reassembled in: 5835]

Client receives the multicast traffic - OTA Captures

FlexConnect Local Switching Mode

The client sends an IGMP Join request to the associated AP. The AP processes the IGMP Join and locally switches the multicast traffic without sending it to the WLC. Multicast traffic flows directly from the wired network to the AP, which then forwards it to interested wireless clients.



Note: Enable IP multicast routing globally, configure PIM on the relevant router interfaces and enable IGMP on the switches between the multicast source and the AP. The WLC does not handle multicast data traffic in this mode.

Related Information

- [Wireless Multicast-Configuration Guide](#)