Wireless Multicast

Wireless multicast

A wireless multicast is a wireless network communication method that

- allows simultaneous transmission of data from a controller to multiple APs and clients
- operates in different modes (unicast and multicast) to accommodate network capabilities and efficiency, and
- leverages features such as IGMP snooping and MGID assignment to optimize multicast traffic delivery.

If the network supports packet multicasting, the multicast method that the controller uses can be configured. The controller performs multicast routing in two modes:

- Unicast mode: The controller unicasts every multicast packet to every AP associated with the controller. Although this mode is inefficient and generates significant extra traffic for the device and the network, it is required on networks that do not support multicast routing. This need arises if the APs are on different subnets than the device's wireless management interface.
- Multicast mode: The controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the controller processor by shifting the work of packet replication to the network. This approach is much more efficient than the unicast method.

The FlexConnect mode has two submodes: local switching and central switching. In local switching mode, data traffic is switched at the AP level and the controller does not process any multicast traffic. In central switching mode, multicast traffic reaches the controller. IGMP snooping, however, takes place at the AP.

When multicast mode is enabled and the controller receives a multicast packet from the wired LAN, it encapsulates the packet using CAPWAP and forwards it to the CAPWAP multicast group address. The controller always uses the management VLAN to send multicast packets. APs in the multicast group receive these packets and forward them to all BSSIDs mapped to the VLAN that delivers multicast traffic to clients.

The controller supports all capabilities of IGMP v1, including multicast listener discovery (MLD) v1 snooping. However, IGMP v2 and IGMP v3 support is limited. This feature tracks and delivers IPv6 multicast flows to clients that request them. For IPv6 multicast, you must enable global multicast mode.

Internet group management protocol (IGMP)

IGMP snooping is a network switch feature that

- listens to IGMP network traffic between hosts and routers
- maintains a map of which devices are subscribed to which multicast groups, and
- forwards multicast traffic only to the relevant devices, reducing unnecessary data transmission.

When this feature is enabled, the controller gathers IGMP reports from clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and VLAN number, and sends the IGMP reports to the IGMP querier. The controller then updates the AP MGID table on the corresponding AP with the client MAC address.

When the controller receives multicast traffic for a particular multicast group, it forwards the traffic to all APs. However, only those APs with active clients subscribed to that multicast group send multicast traffic on the specified WLAN. IP packets are forwarded with an MGID unique to both the ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID unique to the ingress VLAN.

An MGID is a 14-bit value placed in the 16-bit reserved field of wireless information in the CAPWAP header. The remaining two bits must be set to zero.

Multicast optimization

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the device can be configured as a multicast VLAN where multicast groups are registered. Clients can listen to a multicast stream on the multicast VLAN. The system generates the MGID based on both the multicast VLAN and the multicast IP addresses.

- If multiple clients on different VLANs of the same WLAN listen to a single multicast IP address, the system generates a single MGID. The device forwards all multicast streams from clients on this VLAN group through the multicast VLAN. This approach ensures that the upstream router has one entry for all VLANs in the group.
- Only one multicast stream reaches the VLAN group, even when clients are on different VLANs. Therefore, the device sends out just one multicast stream over the network.

Note When VLAN groups are defined and use multicast communication, you must enable the multicast VLAN.

IPv6 global policies

- IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are features provided by IPv6 global policies that you can enable. When you configure ND inspection globally, the policy attributes are stored in the software policy database. You can then apply the policy to an interface. The software policy database updates its entry to record the interface that you applied the policy to.
- The controller enables IPv6 RA guard by default. If Stateless Address Auto-Configuration (SLAAC) is deployed in your network, forward route advertisements (RA) from the wired side to wireless clients.

IPv6 snooping

IPv6 snooping or IPv6 neighbor discovery inspection is a Layer 2 security feature that

- combines several IPv6 first-hop security mechanisms, including IPv6 Address Glean and IPv6 Device Tracking
- learns and secures IPv6 address-to-MAC bindings using neighbor discovery messages, and
- mitigates vulnerabilities such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache in the neighbor discovery process by analyzing and filtering ND protocol traffic based on trusted binding tables

IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, providing IPv6 features with security and scalability.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping can be verified.

When IPv6 ND inspection is configured on a target which can include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, or VLANs (depending on platform support), the device downloads capture instructions to the hardware. These instructions redirect ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are also redirected.

IPv6 ND inspection registers its 'capture rules' with the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL into the platform-dependent modules. When redirected traffic is received, the classifier calls all entry points from registered features for the relevant target, including the IPv6 ND inspection entry point. The IPv6 ND inspection entry point is called last. If another feature makes a decision, such as to drop the traffic, that decision overrides the IPv6 ND inspection action.

IPv6 device tracking

- IPv6 device tracking provides IPv6 host liveness tracking.
- This initiates a neighbor table to immediately update when an IPv6 host disappears.

IPv6 first-hop security binding table

An IPv6 first-hop security binding table is a security database that

- enables the binding table to recover in the event of a device reboot populating from information sources such as neighbor discovery (ND) snooping and DHCP gleaning
- stores entries that map IPv6 neighbors to validate the link-layer addresses (LLA), IPv6 or IPv4 addresses, prefix binding, and
- is used by IPv6 guard features to validate bindings and prevent spoofing or redirect attacks.

The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. When the destination guard cannot resolve a destination address, this feature recovers the missing binding table entries. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery protocols and prefix lists

The IPv6 first-hop security binding table recovery mechanism allows you to configure a prefix list. This list is matched before recovery is attempted for both DHCP and NDP.

- If an address does not match the prefix list associated with the protocol, recovery of the binding table entry with that protocol is not attempted. The prefix list must match the prefixes that are valid for address assignment in the Layer 2 domain for the given protocol.
- By default, no prefix list is configured, so recovery is attempted for all addresses. The command to associate a prefix list to a protocol is **protocol { dhcp | ndp} [prefix-list prefix-list-name]**.

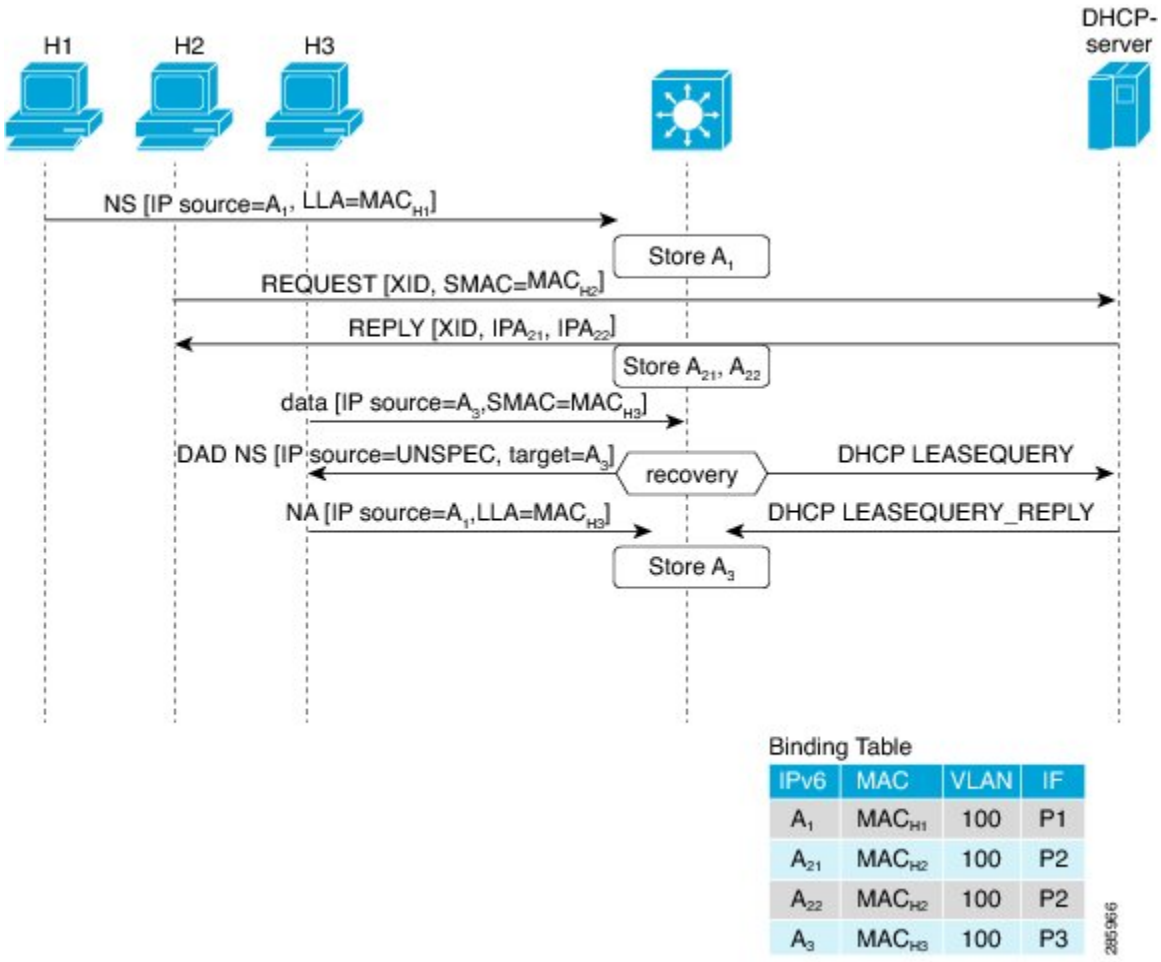
IPv6 address glean

An IPv6 address glean feature is an IPv6 security mechanism that

- inspects Neighbor Discovery (ND) and DHCP messages on a link to discover glean IPv6 addresses
- populates the binding table with gleaned addresses to enable accurate tracking, and
- enforces address ownership, limiting the number of addresses claimed by any node.

This figure shows how IPv6 address glean works.

Figure 1: IPv6 Address Glean



Prerequisites for configuring wireless multicast

IP multicast routing must be enabled and the PIM version and PIM mode must be configured. The default routes should be available in the device. After performing these tasks, the device can forward multicast packets and populate its multicast routing table. To configure multicast mode, the network should be enabled for multicast.

- Multicast hosts, routers, and multilayer switches must have IGMP enabled to participate in IP multicasting.
- When enabling multicast mode on the controller, a CAPWAP multicast group address should also be configured. APs use IGMP to listen to the CAPWAP multicast group.
- You must be cautious when using IGMPv3 with switches 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 if IGMP snooping is disabled or if IGMPv2 is configured on the interface.
- It is recommended to enable IGMPv3 on all intermediate or Layer 3 network devices, especially on each subnet used by multicast devices, such as controller and AP subnets.

Restrictions on configuring wireless multicast

These are the restrictions for configuring IP multicast forwarding:

- APs in monitor mode, sniffer mode, or rogue-detector mode do not join the CAPWAP multicast group address.
- Each controller should be configured with a distinct CAPWAP multicast group.
- Do not enable multicast routing on the management interface.
- Multicast with VLAN groups is supported only in APs operating in local mode.
- The uplink switch should route multicast traffic from wireless clients within a VLAN that is not configured for multicast.
- The wireless multicast to unicast (MCUC) mode is only supported in 9800-CL small template.
- Cisco IOS XE 17.9.5, 17.12.2, 17.14, and later versions support multicast traffic on an AAA-overridden VLAN.
- Multicast-unicast is not supported on large-scale controller appliances, including CW9800L, CW9800M, CW9800H1, and CW9800H2.

Restrictions for IPv6 snooping

The IPv6 snooping feature is not supported on EtherChannel ports.

Configuring wireless multicast

These sections provide information about the various wireless multicast configuration tasks:

Configure wireless multicast-MCMC mode (CLI)

Enable wireless multicast in multicast-over-multicast (MCMC) mode on your device using commands.

Procedure

Step 1 Enable multicast-over-multicast.

Example:

```
Device(config)# wireless multicast 224.0.0.1
```

Use the **no** form of this command to disable the feature.

Step 2 Exit the configuration mode.

Example:

```
Device(config)# end
```

Configure wireless multicast-MCUC mode (CLI)

Enable multicast traffic for wireless clients in MCUC mode using commands.

Note The wireless multicast to unicast (MCUC) mode is only supported in 9800-CL small template.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable multicast traffic for wireless clients.

Example:

```
Device(config)# wireless multicast
```

Step 3 Exit the configuration mode.

Example:

```
Device(config)# end
```

Configure multicast listener discovery snooping (GUI)

Enable or disable multicast listener discovery (MLD) snooping on specific VLANs to efficiently manage multicast network traffic using commands.

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 Click **MLD Snooping**.

Step 3 In the **MLD Snooping** section, click the toggle button to enable or disable MLD snooping.

Step 4 Enter the **MLD Query Interval** in milliseconds. The valid value range is between 100 ms and 32767 ms. The default value is 1000 ms.

Step 5 Move the required VLAN IDs from the **Disabled** section to the **Enabled** section. By default, this feature is disabled on all VLANs.

You can also search for a VLAN ID using the search field. Click **Disable All** to move all the VLAN IDs from the **Enabled** list to the **Disabled** list. Click **Enable All** to move all the VLAN IDs from the **Disabled** list to the **Enabled** list.

Step 6 Click **Apply to Device**.

Configure IPv6 MLD snooping (CLI)

Enable MLD snooping on your device to optimize IPv6 multicast traffic traversal using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# ipv6 mld snooping
```

Step 2 Enable MLD snooping.

Example:

```
Device(config)# ipv6 mld snooping
```

Verify the multicast VLAN configuration

To view the multicast VLAN associated with a policy profile along with the VLAN assigned to that profile, use this command:

```
Device# show wireless profile policy detail default-policy-profile
Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
                Multicast VLAN : 84
Client count                  : 0
Passive Client                : DISABLED
```

To view the multicast VLAN associated with a client, use this command:

```
Device# show wireless client mac ac2b.6e4b.551e detail
Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 192.0.2.20
.........
VLAN : 82
Access VLAN : 82
```

```
Multicast VLAN: 84
```

IPv6 multicast over multicast

A multicast-over-multicast tunnel is a network transmission mechanism that

- enables a wireless controller to efficiently deliver IPv6 multicast traffic to multiple APs simultaneously
- ensures all APs join the same IPv6 multicast address for coordinated data flow, and
- supports deployment in environments where APs may connect via both IPv4 and IPv6 protocols.

When IPv6 multicast over multicast is configured, all APs join the IPv6 multicast address. The multicast traffic from the wireless controller to the APs then flows over the IPv6 multicast tunnel.

The IPv4 APs use a unicast IPv4 CAPWAP tunnel and join the IPv4 multicast group. The IPv6 APs use a unicast IPv6 CAPWAP tunnel and join the IPv6 multicast group.

Note Cisco IOS XE Gibraltar 16.10.1 does not support mixed mode for Multicast over Unicast and Multicast over Multicast over IPv4 and IPv6.

Table 1: Multicast support per platform

Platform	Multicast support - multicast over unicast	Multicast support - multicast over multicast
Cisco Catalyst 9800-40 Wireless Controller	No	Yes
Cisco Catalyst 9800-80 Wireless Controller	No	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Small Template	Yes	Yes
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 IPv6 multicast-over-multicast (GUI)

Enable IPv6 multicast-over-multicast for APs to optimize multicast traffic delivery using the GUI.

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 From the **AP Capwap Multicast** drop-down list, select **Multicast**.

Step 3 Enter the **AP Capwap IPv6 Multicast group Address**.

Step 4 Click **Apply**.

Configure IPv6 multicast-over-multicast (CLI)

Enable IPv6 multicast-over-multicast functionality on your device using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure IPv6 multicast-over-multicast address.

Example:

```
Device(config)# wireless multicast {ipv4 ipv4-address| ipv6 ipv6-address} ff45:1234::86
```

Verify IPv6 multicast-over-multicast

To verify the IPv6 multicast-over-multicast configuration, use these commands:

```
Device# show wireless multicast
Multicast : Enabled
AP Capwap Multicast : Multicast
AP Capwap IPv4 Multicast group Address : 231.1.1.1
AP Capwap IPv6 Multicast group Address : ff45:1234::86
Wireless Broadcast : Disabled
Wireless Multicast non-ip-mcast : Disabled
```

```
Device# show running-configuration | inc multicast
show run | inc multicast:--
wireless multicast
wireless multicast ipv6 ff45:1234::86
wireless multicast 231.1.1.1
```

Verify the multicast connection between the controller and the AP

The Cisco Catalyst 9800 Series Wireless Controller initiates a ping request. This request passes through the CAPWAP multicast tunnel to reach the CAPWAP multicast receiver, which is the AP. In response, the AP sends ping packets to the CAPWAP multicast group IP address and returns the response to the controller.

- View the statistics for transmitted and received traffic on the AP to analyze the data sent through the multicast tunnel.
- To verify multicast tunnel activity, enhance the statistics on the AP. The enhanced statistics show joins, leaves, and data packets transmitted and received through the multicast tunnel.

To confirm if the APs receive multicast to multicast (mom) traffic sent by the controller, use this command:

```
Device# show ap multicast mom
AP Name                     MOM-IP     TYPE MOM- STATUS
-----------------------------------------------------
SS-E-1                      IPv4             Up
SS-E-2                      IPv4             Up
9130E-r3-sw2-g1012          IPv4             Up
9115i-r3-sw2-te1-0-38       IPv4             Up
AP9120-r3-sw3-Gi1-0-46      IPv4             Up
ap3800i-r2-sw1-te2-0-2      IPv4             Up
```

Directed multicast service

A directed multicast service is a wireless networking feature that

- enables APs to transmit multicast packets as unicast frames to clients
- allows clients to reliably receive multicast packets that were missed during sleep mode (for battery savings), and
- improves packet delivery rates and battery life by sending unicast frames at higher wireless link rates.

After receiving this request, an AP buffers multicast traffic for the client. When the client wakes up, the AP transmits the buffered traffic as a unicast frame. The AP can transmit the unicast frames to the client at a higher wireless link rate. Without DMS, the client has to wake up at each Delivery Traffic Indication Map (DTIM) interval to receive multicast traffic.

Configure directed multicast service (GUI)

Enable directed multicast service on a specific WLAN to optimize multicast traffic delivery using the GUI.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLANs** > **Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click on the**Advanced** tab.

Step 4 Check the **Directed Multicast Service** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configure directed multicast service (CLI)

Enable directed multicast service (DMS) on a WLAN to improve multicast efficiency for 802.11v-capable clients using commands.

Before you begin

- This feature is enabled on receiving a request from a client. Make sure to configure this feature under WLAN.
- It is supported only on 802.11v-capable clients, such as Apple iPad and Apple iPhone.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN profile and enter the WLAN profile configuration mode.

Example:

```
Device(config)# wlan test5
```

Step 3 Disable the WLAN profile.

Example:

```
Device(config-wlan)# shutdown
```

Step 4 Configure DMS processing per WLAN.

Example:

```
Device(config-wlan)# dms
```

Step 5 Enable the WLAN profile.

Example:

```
Device(config-wlan)# no shutdown
```

Verify the directed multicast service configuration

To verify the status of the DMS configuration on the controller, use these commands below. The DMS status is displayed under *IEEE 802.11v Parameters*.

```
Device# show wlan id 5
WLAN Profile Name     : test
================================================
Identifier                                : 5
```

```
Network Name (SSID)                             : test
Status                                          : Disabled
Broadcast SSID                                  : Enabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
!
.
.
.
Assisted-Roaming
Neighbor List                                 : Disabled
Prediction List                               : Disabled
Dual Band Support                             : Disabled
! DMS status is displayed below.
IEEE 802.11v parameters
Directed Multicast Service                    : Enabled
BSS Max Idle                                  : Disabled
Protected Mode                                : Disabled
Traffic Filtering Service                     : Disabled
BSS Transition                                : Enabled
Disassociation Imminent                       : Disabled
Optimized Roaming Timer                       : 40
Timer                                         : 200
WNM Sleep Mode                                : Disabled
802.11ac MU-MIMO                              : Disabled
802.11ax parameters
OFDMA Downlink                                : unknown
OFDMA Uplink                                  : unknown
MU-MIMO Downlink                              : unknown
MU-MIMO Uplink                                : unknown
BSS Color                                     : unknown
Partial BSS Color                             : unknown
BSS Color Code
```

To verify the status of the DMS configuration on the controller for clients, use this command:

```
Device# show wireless client mac-address 6c96.cff2.83a0 detail | inc 11v
11v BSS Transition : implemented
11v DMS Capable : Yes
```

To verify the DMS request and response statistics, use this command:

```
Device# show wireless stats client detail | inc DMS
Total DMS requests received in action frame      : 0
Total DMS responses sent in action frame         : 0
Total DMS requests received in Re-assoc Request  : 0
Total DMS responses sent in Re-assoc Response    : 0
```

To verify the DMS configuration Cisco Aironet 2700 and 3700 Series APs, use this command:

```
AP# show controllers dot11Radio 0/1 | begin Global DMS
Global DMS - requests:0 uc:0 drop:408
DMS enabled on WLAN(s): dms-open
 test-open
```

To verify the DMS configuration on the Cisco Aironet 2800, 3800, and 4800 Series APs, use this command:

```
AP# show multicast dms all
 vapid    client              dmsid        TClas
 0       1C:9E:46:7C:AF:C0     1    mask:0x55, version:4, proto:0x11, dscp:0x0, sport:0,
dport:9, sip:0.0.0.0, dip:224.0.0.251
```

Restrictions for wireless broadcast, non-IP multicast and multicast VLAN

Restrictions

- Wireless broadcast does not support VLAN groups.
- If you map a VLAN pool to a WLAN profile, you cannot forward non-IPv4 multicast or broadcast traffic.
- Non-IPv4 multicasts and broadcasts are only available to clients on the VLAN you mapped to the WLAN. You cannot forward them on VLANs defined by AAA override.

Configure non-IP wireless multicast (CLI)

Enable non-IP multicast traffic on wireless VLANs using commands.

Before you begin

- The non-IP Multicast feature is disabled globally by default.
- To allow traffic to pass for non-IP multicast, you must enable global wireless multicast.
- This feature is not supported in Fabric or Flex deployments.

Procedure

Step 1 Enable non-IP multicast in all the VLANs.

Example:

```
Device(config)# wireless multicast non-ip
```

By default, the non-IP multicast in all the VLANs is in disabled state. You must enable wireless multicast for traffic to pass. Use the **no** form of this command to disable non-IP multicast in all the VLANs.

Step 2 Enable non-IP multicast per VLAN.

Example:

```
Device(config)# wireless multicast non-ip vlan 5
```

By default, non-IP multicast per VLAN is disabled. Both wireless multicast and wireless multicast non-IP must be enabled to allow traffic to pass. Use the **no** form of this command to disable non-IP multicast per VLAN.

Step 3 Exit the configuration mode.

Example:

```
Device(config)# end
```

Configure wireless broadcast (GUI)

Enable broadcast packets for wireless clients on selected VLANs using the GUI.

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 On the Multicast page, enable **Wireless Broadcast** to allow packet transmission for wireless clients.

The default value is disabled.

Step 3 In the Disabled VLAN table, click the arrow next to the VLAN ID to change its status from **Disabled** to **Enabled**. This enables broadcast packets for the selected VLAN.

The default value is disabled.

Step 4 Save the configuration.

Configure wireless broadcast (CLI)

Enable wireless clients to receive specific broadcast packets on the network using commands.

Before you begin

- This feature applies only to non-ARP and DHCP broadcast packets.
- By default, the feature is disabled globally.
- The feature is not supported in Fabric or FlexConnect deployments.

Procedure

Step 1 Enable broadcast packets for wireless clients.

Example:

```
Device(config)# wireless broadcast
```

By default, broadcast packets for wireless clients are disabled. When **wireless broadcast** is enabled, broadcast traffic is allowed for each VLAN. Use the **no** form of this command to disable broadcasting packets.

Step 2 Enable broadcast packets for single VLAN.

Example:

```
Device(config)# wireless broadcast vlan 3
```

By default, the Broadcast Packets for a Single VLAN feature is disabled. You must enable wireless broadcast to allow broadcasting. Use the **no** form of this command to disable broadcast traffic for each VLAN.

Step 3 Exit the configuration mode.

Example:

```
Device(config)# end
```

Configure multicast-over-multicast for AP multicast groups (CLI)

Enable multicast-over-multicast to optimize client multicast traffic distribution across APs using commands.

Procedure

Step 1 Configure an all-AP multicast group to send a single packet to all the APs.

Example:

```
Device(config)# ap capwap multicast 239.4.4.4
```

Step 2 Enable multicast-over-multicast for multicasting client multicast group traffic to all the APs through the underlying all-AP multicast group.

Example:

```
Device(config)# wireless multicast 239.4.4.4
```

IP address: Multicast-over-multicast IP address.

Step 3 Exit the configuration mode.

Example:

```
Device(config)# end
```

Verify wireless multicast

- The table provides a comprehensive list of commands for verifying various aspects of wireless multicast, including its general status, IP multicast mode, and mDNS bridging state.

Command	Description
show wireless multicast	Displays the multicast status and IP multicast mode, and each VLAN's broadcast and non-IP multicast status. Also displays the Multicast Domain Name System (mDNS) bridging state.
show wireless multicast group summary	Displays all (Group and VLAN) lists and the corresponding MGID values.
show wireless multicast [**source***source*] **group***group***vlan***vlanid*	Displays details of the specified (S,G,V) and shows all the clients associated with and their MC2UC status.

show ip igmp snooping wireless mcast-spi-count	Displays statistics of the number of multicast SPIs per MGID sent between IOS and the Wireless Controller Module. feature-id [] Displays statistics of the number of multicast SPIs per MGID sent internally between IOS and the Wireless Controller Module. feature-id []
show ip igmp snooping wireless mcast-ipc-count	Displays the number of multicast IPCs per MGID sent to the wireless controller module.
show ip igmp snooping wireless mgid	Displays the MGID mappings.
show ip igmp snooping igmpv2-tracking	Displays the client-to-SGV mappings and the SGV-to-client mappings.
show ip igmp snooping querier vlan*vlanid*	Displays the IGMP querier information for the specified VLAN.
show ip igmp snooping querier detail	Displays the detailed IGMP querier information of all the VLANs.
show ipv6 mld snooping querier vlan*vlanid*	Displays the MLD querier information for the specified VLAN.
show ipv6 mld snooping wireless mgid	Displays MGIDs for the IPv6 multicast group.

Multicast optimization

Previously, multicast was based on a combination of multicast addresses and VLANs, grouped together as a single entity called MGID. Using the VLAN group can lead to an increase in duplicate packets. When the VLAN group feature is enabled, each client listens to the multicast stream on a different VLAN. As a result, the device creates a separate MGID for each multicast address and VLAN. Consequently, the upstream router sends one copy per VLAN, resulting in a number of copies equal to the number of VLANs in the group. Since all clients use the same WLAN, multiple copies of the multicast packet are sent across the wireless network. The multicast optimization feature suppresses duplication of multicast streams on the wireless medium between the device and the APs.

- This feature enables you to create a multicast VLAN for multicast traffic. You can configure one of the VLANs in the device as a multicast VLAN, where multicast groups are registered. Clients can listen to a multicast stream on the multicast VLAN. The MGID is generated based on the multicast VLAN and multicast IP addresses.
- If multiple clients on different VLANs within the same WLAN listen to a single multicast IP address, the device generates a single MGID. The device ensures that all multicast streams from clients in the VLAN group are sent via the multicast VLAN. This approach allows the upstream router to use a single entry for all VLANs in the VLAN group. Only one multicast stream is sent to the VLAN group, even when clients are on different VLANs. As a result, the device sends only one multicast stream over the network.

Configure IP multicast VLAN for WLAN (GUI)

Configure an IP multicast VLAN for a Wireless LAN to enable efficient multicast traffic delivery using the GUI.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** and **Description**.

Step 4 Enable the **Central Switching** and **Central Association** toggle buttons.

Step 5 In the **Access Policies** tab, under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list and enter the **Multicast VLAN**.

Step 6 Click **Apply to Device**.

Configure IP multicast VLAN for WLAN (CLI)

Set up IP multicast VLAN for WLAN to enable both IPv4 and IPv6 multicast forwarding to APs using commands.

Before you begin

- This feature is not supported in Fabric or FlexConnect deployments.
- Multicast VLAN is used for both IPv4 and IPv6 multicast forwarding to APs.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure WLAN policy profile and enter the wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy default-policy-profile
```

Step 3 Configure central association for locally switched clients.

Example:

```
Device(config-wireless-policy)# central association
```

Step 4 Configure WLAN for central switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 5 (Optional) Add a description for the policy profile.

Example:

```
Device(config-wireless-policy)# description test
```

Step 6 Assign the profile policy to the VLAN.

Example:

```
Device(config-wireless-policy)# vlan 32
```

Step 7 Configure multicast for the VLAN.

Example:

```
Device(config-wireless-policy)# multicast vlan 84
```

Step 8 Enable the profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Verify the multicast VLAN configuration

To view the multicast VLAN associated with a policy profile along with the VLAN assigned to that profile, use this command:

```
Device# show wireless profile policy detail default-policy-profile
Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
                Multicast VLAN : 84
Client count                  : 0
Passive Client                : DISABLED
```

To view the multicast VLAN associated with a client, use this command:

```
Device# show wireless client mac ac2b.6e4b.551e detail
Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 192.0.2.20
…….
VLAN : 82
Access VLAN : 82
                Multicast VLAN: 84
```

Multicast Filtering

Multicast filtering

A multicast filter is a wireless network feature that

- selectively controls the acceptance or dropping of multicast group membership requests from wireless clients

- supports configuration per WLAN for both IPv4 (using IGMP) and IPv6 (using MLD), and
- prevents addition of unauthorized clients to AP multicast groups by filtering protocol-specific reports.

The multicast filtering feature is disabled by default. You can enable or disable the multicast filtering feature per WLAN, from the controller.

You can enable or disable the multicast filtering feature per WLAN from the controller. When you enable this feature, the APs drop the internet group management protocol (IGMP) join request from any client that is part of the WLAN and attempts to join a Layer 3 multicast group address. When you disable this feature, the APs honor the IGMP join request from clients that are part of the WLAN.

This table shows AP behavior for IPv4 and IPv6:

Table 2: Multicast filtering per WLAN

Multicast filtering feature status	IPv4	IPv6
Enabled	AP drops the internet group management protocol (IGMP) membership report from a client that is a part of a WLAN.	AP drops the multicast listener discovery (MLD) report with multicast group address scope value greater than three from a client that is a part of a WLAN.
Disabled	AP honors the IGMP membership report from the client that is a part of a WLAN.	AP honors the MLD report from the client that is a part of a WLAN

Feature history for multicast filtering

- This table provides release and related information for the feature explained in this module.
- This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 3: Feature history for multicast filtering

Feature name	Release information	Feature description
Multicast filtering	Cisco IOS XE 17.3.1	From this release, the multicast filtering feature is supported on Layer 3 for IPv6.
Multicast filtering	Cisco IOS XE 17.2.1	From this release, the multicast filtering feature is supported on Layer 3 for IPv4.

Supported L3 multicast report for filtering

APs drop IGMP and MLD join requests from clients on the WLAN for any Layer 3 multicast group address, based on these filtering options:

- IPv4: IGMP versions to be filtered:
  - V1 membership report (0x12)

- V2 membership report (0x16)
- V3 membership report (0x22)

- IPv6: ICMPv6 types to be filtered, except link-local multicast packets:
  - Multicast Listener report: MLD Version 1 (131)
  - Multicast Listener report: MLD Version 2 (143)

Note Filtering supported types prevents creating or adding a client entry to the AP multicast group table.

Configure multicast filtering (CLI)

Enable multicast filtering to control the flow of multicast traffic on a specific WLAN using commands.

Perform the procedure given here to create a policy profile and then enable Multicast Filtering on a WLAN:

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a WLAN policy profile and enter the wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy rr-xyz-policy-1
```

Step 3 Configure a multicast filter.

Example:

```
Device(config-wireless-policy)#multicast filter
```

Use the **no** form of this command to disable the feature.

What to do next

1. Create a policy tag. For more information about creating policy tags, see *Configuring a Policy Tag (CLI)*.
2. Map the policy tag to an AP. For more information about mapping a policy tag to an AP, see *Attaching a Policy Tag and Site Tag to an AP (CLI)*.

Verify multicast filtering

To verify if multicast filtering is enabled, use the **show wireless profile policy detailed** *named-policy-profile* command:

```
Device# show wireless profile policy detailed named-policy-profile
Policy Profile Name                : named-policy-profile
Description                        :
Status                             : DISABLED
VLAN                               : 91
Multicast VLAN                     : 0
OSEN client VLAN                   :
Multicast Filter                   : ENABLED
```