Wireless Multicast

Information About Wireless Multicast

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 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 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 and shifts the work of packet replication to the network, which is much more efficient than the unicast method.

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

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.

The controller supports all the capabilities of IGMP v1, including Multicast Listener Discovery (MLD) v1 snooping, but the IGMP v2 and IGMP v3 capabilities are limited. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, global multicast mode should be enabled.

Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the controller snooping gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the IGMP querier. The controller then updates the access-point MGID table on the corresponding access point with the client MAC address. When the controller receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress VLAN.

MGID is a 14-bit value filled in the 16-bit reserved field of wireless information in the CAPWAP header. The remaining two bits should 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. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the multicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The device makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Note When VLAN groups are defined and uses multicast communication, then you need to 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 IPv6 global policies features. Every time an ND inspection is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA guard is enabled by default on the controller. RA from the wired side should be forwarded to the wireless clients if the Stateless Address Auto-Configuration (SLAAC) is deployed in the network.

Information About IPv6 Snooping

The following sections provide information about IPv6 snooping.

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism,

such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order 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 is verifiable. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up 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 redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. 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. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. 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 feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

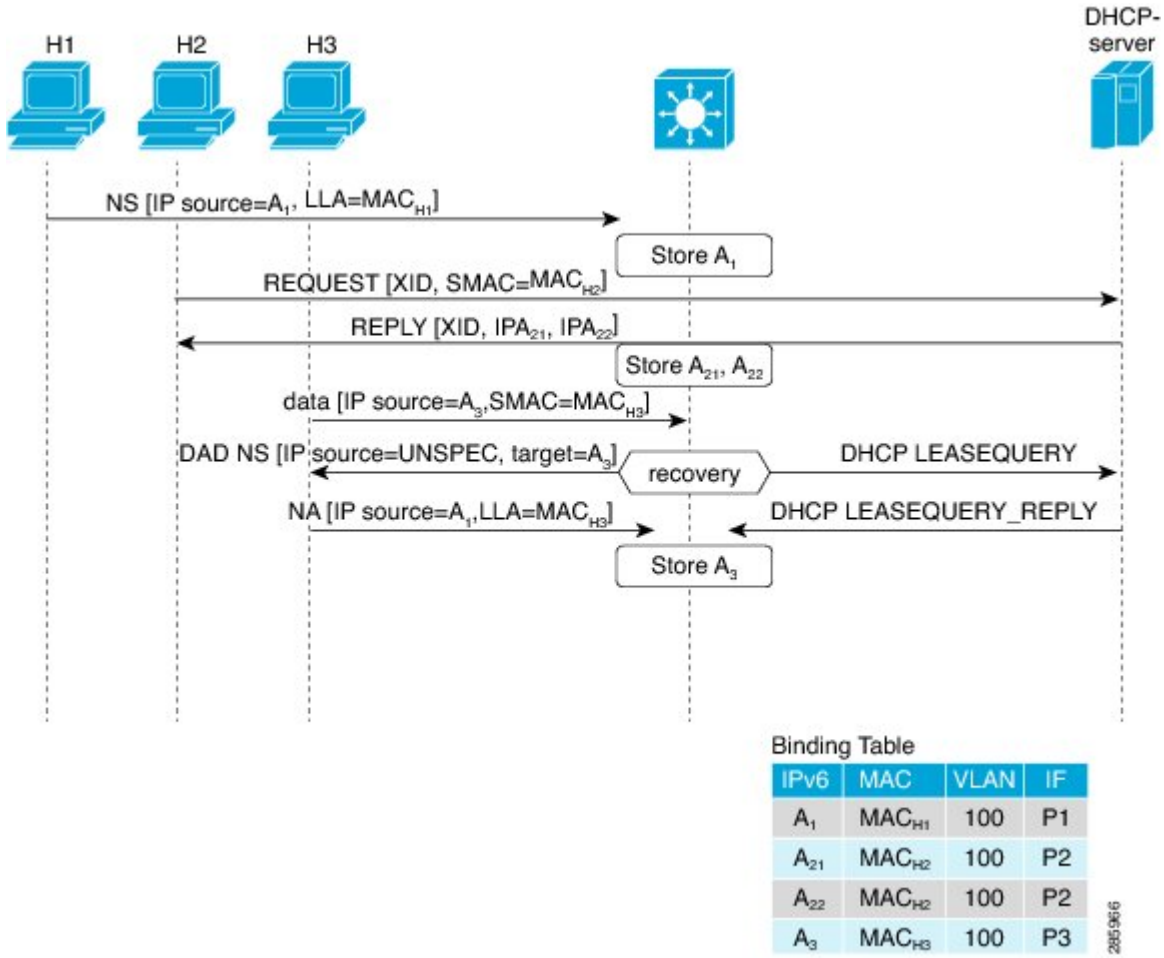
If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the 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

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

The following figure shows how IPv6 address glean works.

Figure 1: IPv6 Address Glean



Prerequisites for Configuring Wireless Multicast

- To participate in IP multicasting, the multicast hosts, routers, and multilayer switches must have IGMP operating.
- When enabling multicast mode on the controller, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.

- 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.

Restrictions on Configuring Wireless Multicast

The following are the restrictions for configuring IP multicast forwarding:

- Access points in monitor mode, sniffer mode, or rogue-detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the controllers should be different for different controllers.
- Multicast routing should not be enabled for the management interface.
- Multicast with VLAN group is only supported in local mode AP.
- Multicast traffic from wireless clients in non-multicast VLAN should be routed by the uplink switch.
- Multicast traffic on an AAA overridden VLAN is not supported.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on EtherChannel ports.

Configuring Wireless Multicast

The following sections provide information about the various wireless multicast configuration tasks:

Configuring Wireless Multicast-MCMC Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless multicast***ip-addr* **Example:** `Device(config)# wireless multicast 231.1.1.1`	Enables multicast-over-multicast. Use the **no** form of this command to disable the feature.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Wireless Multicast-MCUC Mode

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enables the multicast traffic for wireless clients. By default, the feature is in disabled state. Use the **no** form of this command to disable the multicast traffic for wireless clients and disable mDNS bridging.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Multicast Listener Discovery Snooping (GUI)

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 value range is between 100 ms and 32767 ms. The default value is 1000 ms.

Step 5 Move the required VLAN IDs listed in the **Disabled** section to the **Enabled** section. (By default, this feature is disabled on the VLAN.)

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

Step 6 Click **Apply to Device**.

Configuring IPv6 MLD Snooping

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# ipv6 mld snooping`	Enters global configuration mode.
Step 2	**ipv6 mld snooping** **Example:** `Device(config)# ipv6 mld snooping`	Enables MLD snooping.

Verifying the Multicast VLAN Configuration

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

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
…….
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

IPv6 Multicast-over-Multicast

IPv6 multicast allows a host to send a single data stream to a subset of all the hosts (group transmission) simultaneously. When IPv6 Multicast over Multicast is configured, all the APs join the IPv6 multicast address, and the multicast traffic from the wireless controller to the AP flows over the IPv6 multicast tunnel.

In mixed deployments (IPv4 and IPv6), the APs might join the wireless controller over IPv4 or IPv6. To enable Multicast over Multicast in mixed deployments, configure both IPv4 and IPv6 multicast tunnels. The IPv4 APs have a unicast IPv4 CAPWAP tunnel and join the IPv4 multicast group. The IPv6 APs will have a unicast IPv6 CAPWAP tunnel and joins the IPv6 multicast group.

Note Mixed mode of Multicast over Unicast and Multicast over Multicast over IPv4 and IPv6 is not supported in Cisco IOS XE Gibraltar 16.10.1.

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

Configuring IPv6 Multicast-over-Multicast (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**.

Configuring IPv6 Multicast-over-Multicast

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** {*ipv4-address* | **ipv6** *ipv6-address*) **Example:** `Device(config)# wireless multicast ipv6 ff45:1234::86`	Configures IPv6 multicast-over-multicast address.

Verifying IPv6 Multicast-over-Multicast

To verify the IPv6 multicast-over-multicast configuration, use the following 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
```

Verifying the Multicast Connection Between the Controller and the AP

Cisco Catalyst 9800 Series Wireless Controller initiates a ping request that passes through the CAPWAP multicast tunnel onto the CAPWAP multicast receiver, which is the AP. In response, the AP pings the packets for CAPWAP multicast group IP address, and sends back the response to the controller. You can view the statistics on the AP for transmitted and received traffic to analyze the data that are sent and received through the multicast tunnel. Alternatively, you can also verify by enhancing the existing statistics on the AP for transmitted and received traffic to explicitly list the joins, leaves, 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 the following 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

The Directed Multicast Service (DMS) feature allows a client to request access points (AP) to transmit multicast packets as unicast frames. After receiving this request, an AP buffers the multicast traffic for a client and transmits it as a unicast frame when the client wakes up. This allows the client to receive the multicast packets that were ignored while in sleep mode (to save battery power) and also ensures Layer 2 reliability. The unicast frames are transmitted to the client at a potentially higher wireless link rate, which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus saving more battery power. Without DMS, the client has to wake up at each Delivery Traffic Indication Map (DTIM) interval to receive multicast traffic.

Configuring Directed Multicast Service(GUI)

Procedure

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

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

Step 3 Click **Advanced** tab.

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

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

Configuring Directed Multicast Service

Before you begin

- This feature is enabled on receiving a request from a client. Ensure that this feature is configured under WLAN.
- This feature is supported only on 802.11v-capable clients, such as Apple iPad and Apple iPhone.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test5`	Configures the WLAN profile and enters WLAN profile configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN profile.
Step 4	**dms** **Example:** `Device(config-wlan)# dms`	Configures DMS processing per WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN profile.

Verifying the Directed Multicast Service Configuration

To verify the status of the DMS configuration on the controller, use **show** 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 the following 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 the following 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 the following 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 the following 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
```

Wireless Broadcast, Non-IP Multicast and Multicast VLAN

Restrictions

- Wireless broadcast does not support VLAN groups.
- When a VLAN pool is mapped to the WLAN profile, support for forwarding non-IPv4 multicast and broadcast is unavailable.
- Non-IPv4 multicasts and broadcasts are restricted to clients on the VLAN mapped to the WLAN and are not forwarded on VLANs returned by AAA override.

Configuring Non-IP Wireless Multicast (CLI)

Before you begin

- The non-IP Multicast feature is disable globally, by default.
- For non-IP multicast, global wireless multicast must be enabled for traffic to pass.
- This feature is not supported in Fabric or Flex deployments.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast non-ip** **Example:** `Device(config)# wireless multicast non-ip`	Enables non-IP multicast in all the VLANs. By default, the non-IP multicast in all the VLANs is in Disabled state. Wireless multicast must be enabled for the traffic to pass. Use the **no** form of this command to disable non-IP multicast in all the VLANs.
Step 3	**wireless multicast non-ip vlan** *vlanid* **Example:** `Device(config)# wireless multicast non-ip vlan 5`	Enables non-IP multicast per VLAN. By default, non-IP multicast per VLAN is in Disabled state. Both wireless multicast and wireless multicast non-IP must be enabled for traffic to pass. Use the **no** form of this command to disable non-IP multicast per VLAN.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Wireless Broadcast (GUI)

Procedure

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

Step 2 In the Multicast page, change the status of the **Wireless Broadcast** to enabled to broadcast packets for wireless clients.

The default value is disabled.

Step 3 From the Disabled VLAN table, click the arrow adjacent to the VLAN ID in the **Disabled** state to the **Enabled** state to enable broadcast packets for a VLAN.

The default value is disabled.

Step 4 Save the configuration.

Configuring Wireless Broadcast (CLI)

Before you begin

- This feature is applicable only to non-ARP and DHCP broadcast packets.
- This feature is disable globally, by default.
- This feature is not supported in Fabric or Flex deployments.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless broadcast** **Example:** `Device(config)# wireless broadcast`	Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in Disabled state. Enabling **wireless broadcast** enables broadcast traffic for each VLAN. Use the **no** form of this command to disable broadcasting packets.
Step 3	**wireless broadcast vlan** *vlanid* **Example:** `Device(config)# wireless broadcast vlan 3`	Enables broadcast packets for single VLAN. By default, the Broadcast Packets for a Single VLAN feature is in Disabled state. Wireless broadcast must be enabled for broadcasting. Use the **no** form of this command to disable broadcast traffic for each VLAN.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Multicast-over-Multicast for AP Multicast Groups (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap capwap multicast** *IP address* **Example:** `Device(config)# ap capwap multicast 239.4.4.4`	Configures an all-AP multicast group to send a single packet to all the APs.
Step 3	**wireless multicast** *IP address* **Example:** `Device(config)# wireless multicast 239.4.4.4`	Enables Multicast-over-Multicast for multicasting client multicast group traffic to all the APs through the underlying all-AP multicast group. *IP address*—Multicast-over-multicast IP address.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Verifying Wireless Multicast

Table 2: Commands for Verifying Wireless Multicast

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-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.

Command	Description
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

Multicast used to be based on the group of the multicast addresses and the VLAN as one entity, MGID. With the VLAN group, duplicate packets might increase. Using the VLAN group feature, every client listens to the multicast stream on a different VLAN. As a result, the device creates different MGIDs for each multicast address and the VLAN. Therefore, the upstream router sends a copy for each VLAN, which results in as many copies as the number of VLANs in the group. Because the WLAN remains the same for all the clients, multiple copies of the multicast packet are sent over the wireless network. To suppress the duplication of a multicast stream on the wireless medium between the device and the access points, the multicast optimization feature can be used.

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. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the multicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The device makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Configuring IP Multicast VLAN for WLAN (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**.

Configuring IP Multicast VLAN for WLAN

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 5	**description** *policy-profile-name* **Example:** `Device(config-wireless-policy)# description "test"`	(Optional) Adds a description for the policy profile.
Step 6	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 7	**multicast vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# multicast vlan 84`	Configures multicast for the VLAN.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Verifying the Multicast VLAN Configuration

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

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
……..
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

Multicast Filtering

Information About Multicast Filtering

In Cisco IOS XE Amsterdam, Release 17.2.1, the Multicast Filtering feature is supported on Layer 3 for IPv4.

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 a client that is part of the WLAN, for any Layer 3 multicast group address. When you disable this feature, the APs honor the IGMP join request from the client that is part of the WLAN.

In the Cisco IOS XE Amsterdam, Release 17.3.1, the Multicast Filtering feature is supported on Layer 3 for IPv6.

You can enable or disable the Multicast Filtering feature per WLAN, from the controller. The following table shows the AP behavior with IPv4 and IPv6:

The Multicast Filtering feature is disabled by default.

Table 3: 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.

Multicast Filtering Feature Status	IPv4	IPv6
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.

Supported L3 Multicast Report for Filtering

APs will not honor and drop IGMP and MLD join requests from a client part of WLAN for any L3 multicast group address as per the below 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 of supported types will prevent the creation or addition of a client entry to the AP multicast group table.

Configuring Multicast Filtering

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

Before you begin

Create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**multicast filter** **Example:** `Device(config-wireless-policy)#multicast filter`	Configures a 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)*.

Verifying 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
```