Multicast/Broadcast Setup

Configuring Multicast Mode

Information About Multicast/Broadcast Mode

If your network supports packet multicasting, you can configure the multicast method that the controller uses. The controller performs multicasting in two modes:

- Unicast mode—In this mode, the controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient but might be required on networks that do not support multicasting.
- Multicast mode—In this mode, the controller sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

When you enable multicast mode 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 interface for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the interface on which clients receive multicast traffic. From the access point perspective, the multicast appears to be a broadcast to all SSIDs.

Note Until Release 7.5, the port number used for CAPWAP multicast was 12224. From Release 7.6 onwards, the port number used for CAPWAP is changed to 5247.

The controller supports Multicast Listener Discovery (MLD) v1 snooping for IPv6 multicast. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, you must enable Global Multicast Mode.

Note When you disable the Global Multicast Mode, the controller still forwards the IPv6 ICMP multicast messages, such as router announcements and DHCPv6 solicits, as these are required for IPv6 to work. As a result, enabling the Global Multicast Mode on the controller does not impact the ICMPv6 and the DHCPv6 messages. These messages will always be forwarded irrespective of whether or not the Global Multicast Mode is enabled.

Internet Group Management Protocol (IGMP) snooping is available to better direct multicast packets. When this feature is enabled, the controller gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) from the IGMP reports after selecting the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the infrastructure switch. The controller sends these reports with the source address as the interface address on which it received the reports from the clients. The controller then updates the access point MGID table on the 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 interface.

When IGMP snooping is disabled, the following is true:

- The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned one Layer 2 MGID. For example, the management interface has an MGID of 0, and the first dynamic interface created is assigned an MGID of 8, which increments as each dynamic interface is created.
- The IGMP packets from clients are forwarded to the router. As a result, the router IGMP table is updated with the IP address of the clients as the last reporter.

When IGMP snooping is enabled, the following is true:

- The controller always uses Layer 3 MGID for all Layer 3 multicast traffic sent to the access point. For all Layer 2 multicast traffic, it continues to use Layer 2 MGID.
- IGMP report packets from wireless clients are consumed or absorbed by the controller, which generates a query for the clients. After the router sends the IGMP query, the controller sends the IGMP reports with its interface IP address as the listener IP address for the multicast group. As a result, the router IGMP table is updated with the controller IP address as the multicast listener.
- When the client that is listening to the multicast groups roams from one controller to another, the first controller transmits all the multicast group information for the listening client to the second controller. As a result, the second controller can immediately create the multicast group information for the client. The second controller sends the IGMP reports to the network for all multicast groups to which the client was listening. This process aids in the seamless transfer of multicast data to the client.
- If the listening client roams to a controller in a different subnet, the multicast packets are tunneled to the anchor controller of the client to avoid the reverse path filtering (RPF) check. The anchor then forwards the multicast packets to the infrastructure switch.

Note The MGIDs are controller specific. The same multicast group packets coming from the same VLAN in two different controllers may be mapped to two different MGIDs.

Note If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses coming from an interface.

Note The number of multicast addresses supported per VLAN for a Cisco WLC is 100.

Restrictions on Configuring Multicast Mode

- The Cisco Wireless network solution uses some IP address ranges for specific purposes, and you should keep these ranges in mind when configuring a multicast group:
  - 224.0.0.0 through 224.0.0.255—Reserved link local addresses
  - 224.0.1.0 through 238.255.255.255—Globally scoped addresses
  - 239.0.0.0 through 239.255.x.y /16—Limited scope addresses
- When you enable multicast mode on the Cisco WLC, you must also configure a CAPWAP multicast group address. APs subscribe to the CAPWAP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3.
- APs 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.
- Lightweight APs transmit multicast packets at the highest configured mandatory data rate.

  Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell might fail to receive them successfully. If reliable reception is a goal, multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, it might be useful to shrink the cell size and disable all lower data rates.

  Depending on your requirements, you can take the following actions:
  - If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, that is low enough to reach the edges of the wireless cells.
  - If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, you can configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of nonmulticast clients.
- Multicast mode does not operate across intersubnet mobility events such as guest tunneling. It does, however, operate with interface overrides using RADIUS (but only when IGMP snooping is enabled) and with site-specific VLANs (access point group VLANs).
- For LWAPP, the controller drops multicast packets sent to UDP control port 12223. For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively. Therefore, you may want to consider not using these port numbers with the multicast applications on your network.

- We recommend that any multicast applications on your network not use the multicast address configured as the CAPWAP multicast group address on the controller.
- For multicast to work on Cisco 2504 WLC, you have to configure the multicast IP address.
- Multicast mode is not supported on Cisco Flex 7500 Series WLCs.
- IGMP and MLD snooping is not supported on Cisco Flex 7510 WLCs.
- For Cisco 8510 WLCs:
  - You must enable multicast-unicast if IPv6 support is required on FlexConnect APs with central switching clients.
  - You can change from multicast mode to multicast-unicast mode only if global multicast is disabled, which means IGMP or MLD snooping is not supported.
  - FlexConnect APs do not associate with a multicast-mulitcast group.
  - IGMP or MLD snooping is not supported on FlexConnect APs. IGMP and MLD snooping is allowed only for local mode APs in multicast-multicast mode.
  - Because VideoStream requires IGMP or MLD snooping, the VideoStream feature works only on local mode APs if multicast-multicast mode and snooping are enabled.
- In a multicast group, when multicast audio is initiated, the recipients do not hear the first two seconds of the multicast audio. As a workaround, we recommend that you set the Cisco APs to FlexConnect + Local Switching mode for small-scale deployments.
- To reduce join latency, we recommend disabling IPv6 on the Cisco WLC.
- FlexConnect APs do not join the multicast group when the Multicast mode is Multicast-Multicast and CAPWAP has IPv4 and IPv6. For Cisco 5508 and 8510 WLCs, you can disable the Multicast-Multicast mode and enable the Multicast-Unicast mode. For Cisco Flex 7510 WLC, there is no Multicast-Multicast configuration. For FlexConnect APs in Multicast-Multicast mode joined with central switching clients, there is reduction of 0-13 percent in data throughput.
- We recommend that you do not use Broadcast-Unicast or Multicast-Unicast mode on Cisco WLC setup where there are more than 50 APs connected together.

  If a Cisco WLC setup has more than 50 APs, the CAPWAP control messages between Cisco WLC and AP may be delayed due to duplication of each Multicast or Broadcast traffic to each of the APs. The delay in the CAPWAP control messages causes client association or 802.1X authentication to be delayed for 1 to 3 seconds. As a result of this, the client receives repeated authentication prompts or failure messages.
- While using Local and FlexConnect AP mode the Cisco WLC's multicast support differs for different platforms.

  The parameters that affect Multicast forwarding are:
  - Cisco WLC platform.
  - Global AP multicast mode configuration at Cisco WLC.
  - Mode of the AP—Local, FlexConnect central switching.
  - For Local switching, it does not send/receive the packet to/from Cisco WLC, so it does not matter which Multicast mode is configured on the Cisco WLC.

Note FlexConnect mode AP cannot join Multicast group address configured at Cisco WLC. Therefore, the FlexConnect mode AP cannot receive Multicast packets that are sent by Cisco WLC (Multicast packets sent by FlexConnect central switching is received by local mode APs). If Multicast needs to be forwarded for FlexConnect central switching, you must configure AP mode as Multicast to Unicast. This configuration is global because it is applicable to local mode AP.

- Effective with Release 8.2.100.0, it is not possible to download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations introduced in this release. The platform support for global multicast and multicast mode are listed in the following table.

Table 1: Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Supported
Cisco 5520 , 8510, and 8540 WLCs	Enabled	Unicast	No
	Enabled	Multicast	Yes
	Disabled	Unicast	No mulitcast support (config supported)
	Disabled	Multicast	No mulitcast support (config supported)
Cisco Flex 7510 WLC	Global Multicast cannot be enabled. Only Unicast mode is supported. Also, AP-Multicast mode cannot be changed to Multicast-Multicast.		
Cisco 2504 WLC	Only Multicast mode is supported.		
Cisco vWLC	Multicast is not supported; only Unicast mode is supported.		
and Cisco 5508 WLC	Enabled	Unicast	Yes
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No

Enabling Multicast Mode (GUI)

Step 1 Choose **Controller** > **Multicast** to open the Multicast page.

Step 2 Select the **Enable Global Multicast Mode** check box to configure sending multicast packets. The default value is disabled.

Note FlexConnect supports unicast mode only.

Step 3 If you want to enable IGMP snooping, select the **Enable IGMP Snooping** check box. If you want to disable IGMP snooping, leave the check box unselected. The default value is disabled.

Step 4 To set the IGMP timeout, enter a value between 30 and 7200 seconds in the IGMP Timeout text box. The controller sends three queries in one timeout value at an interval of *timeout*/ 3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enter the IGMP Query Interval (seconds).

Step 6 Select the **Enable MLD Snooping** check box to support IPv6 forwarding decisions.

Note To enable MLD Snooping, you must enable Global Multicast Mode of the controller.

Step 7 In the **MLD Timeout** text box, enter a value between 30 and 7200 seconds to set the MLD timeout.

Step 8 Enter the MLD Query Interval (seconds). The valid range is between 15 and 2400 seconds.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Enabling Multicast Mode (CLI)

Step 1 Enable or disable multicasting on the controller by entering this command:
config network multicast global {**enable** | **disable**}

The default value is disabled.

Note The **config network broadcast** {**enable** | **disable**} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode currently on the controller to operate.

Step 2 Perform either of the following:

a) Configure the controller to use the unicast method to send multicast packets by entering this command:
config network multicast mode unicast

b) Configure the controller to use the multicast method to send multicast packets to a CAPWAP multicast group by entering this command:
config network multicast mode multicast *multicast_group_ip_address*

Step 3 Enable or disable IGMP snooping by entering this command:
config network multicast igmp snooping {**enable** | **disable**}

The default value is disabled.

Step 4 Set the IGMP timeout value by entering this command:
config network multicast igmp timeout *timeout*

You can enter a *timeout* value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of *timeout*/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enable or disable Layer 2 Multicast by entering this command:
config network multicast l2mcast {**enable** {**all** | *interface-name*} | **disable**}

Step 6 Enable or disable MLD snooping by entering this command:
config network multicast mld snooping {**enable** | **disable**}

The default value is disabled.

Note To enable MLD snooping, you must enable global multicast mode of the controller.

Step 7 Set the MLD timeout value by entering this command:
config network multicast mld timeout *timeout*

Enter the MLD Query Interval (seconds). The valid range is between 15 and 2400 seconds.

Step 8 Save your changes by entering this command:
save config

Viewing Multicast Groups (GUI)

Step 1 Choose **Monitor > Multicast**. The Multicast Groups page appears.
This page shows all the multicast groups and their corresponding MGIDs.

Step 2 Click the link for a specific MGID (such as MGID 550) to see a list of all the clients joined to the multicast group in that particular MGID.

Viewing Multicast Groups (CLI)

Before You Begin

- See all the multicast groups and their corresponding MGIDs by entering this command:

show network multicast mgid summary

Information similar to the following appears:

```
Layer2 MGID Mapping:
--------------------
InterfaceName                    vlanId   MGID
-------------------------------- ------   ----
management                       0        0
test                             0        9
wired                            20       8

Layer3 MGID Mapping:
--------------------
Number of Layer3 MGIDs.......................... 1

 Group address    Vlan  MGID
 ---------------  ----  ----
 239.255.255.250  0     550
```

- See all the clients joined to the multicast group in a specific MGID by entering this command:

  show network multicast mgid detail *mgid_value*

  where the *mgid_value* parameter is a number between 550 and 4095.

  Information similar to the following appears:

```
Mgid.......................................... 550
Multicast Group Address..................... 239.255.255.250
Vlan.......................................... 0
Rx Packet Count............................... 807399588
No of clients................................. 1
Client List..................................
        Client MAC            Expire Time (mm:ss)
        00:13:02:23:82:ad     0:20
```

Viewing an Access Point's Multicast Client Table (CLI)

To help troubleshoot roaming events, you can view an access point's multicast client table from the controller by performing a remote debug of the access point.

Step 1 Initiate a remote debug of the access point by entering this command:
debug ap enable *Cisco_AP*

Step 2 See all of the MGIDs on the access point and the number of clients per WLAN by entering this command:
debug ap command "**show capwap mcast mgid all**" *Cisco_AP*

Step 3 See all of the clients per MGID on the access point and the number of clients per WLAN by entering this command:
debug ap command "**show capwap mcast mgid id** *mgid_value*" *Cisco_AP*

Mediastream

Information about VideoStream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable.

The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each VideoStream client acknowledges receiving a video IP multicast stream.

Prerequisites for VideoStream

Make sure that the multicast feature is enabled. We recommend configuring IP multicast on the controller with multicast-multicast mode.

Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.

Verify that the access points have joined the controllers.

Make sure that the clients are able to associate to the configured WLAN at 802.11n speed.

Restrictions for Configuring VideoStream

VideoStream is supported in the 7.0.98.0 and later controller software releases.

The Cisco OEAP-600 does not support VideoStream. All other access points support VideoStream.

Configuring VideoStream (GUI)

Step 1 Configure the multicast feature by following these steps:

a) Choose **Wireless** > **MediaStream** > **General**.

b) Select or unselect the **Multicast Direct feature** check box. The default value is disabled.

Note Enabling the multicast direct feature does not automatically reset the existing client state. The wireless clients must rejoin the multicast stream after enabling the multicast direct feature on the controller.

c) In the **Session Message Config** area, select **Session announcement State** check box to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.

d) In the **Session announcement URL** text box, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

e) In the **Session announcement e-mail** text box, enter the e-mail address of the person who can be contacted.

f) In the **Session announcement Phone** text box, enter the phone number of the person who can be contacted.

g) In the **Session announcement Note** text box, enter a reason as to why a particular client cannot be served with a multicast media.
h) Click **Apply**.

Step 2 Add a media stream by following these steps:

a) Choose **Wireless** > **Media Stream** > **Streams** to open the Media Stream page.
b) Click **Add New** to configure a new media stream. The **Media Stream > New** page appears.
Note The Stream Name, Multicast Destination Start IP Address (IPv4 or IPv6), and Multicast Destination End IP Address (IPv4 or IPv6) text boxes are mandatory. You must enter information in these text boxes.
c) In the **Stream Name** text box, enter the media stream name. The stream name can be up to 64 characters.
d) In the **Multicast Destination Start IP Address (IPv4 or IPv6)** text box, enter the start (IPv4 or IPv6) address of the multicast media stream.
e) In the **Multicast Destination End IP Address (IPv4 or IPv6)** text box, enter the end (IPv4 or IPv6) address of the multicast media stream.
Note Ensure that the Multicast Destination Start and End IP addresses are of the same type, that is both addresses should be of either IPv4 or IPv6 type.
f) In the **Maximum Expected Bandwidth** text box, enter the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 kbps.
Note We recommend that you use a template to add a media stream to the controller.
g) From the **Select from Predefined Templates** drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify the details about the resource reservation control:

- Very Coarse (below 300 kbps)
- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)
- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

Note When you select a predefined template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

- Average Packet Size (100-1500 bytes)—Specifies the average packet size. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
- RRC Periodic update—Enables the RRC (Resource Reservation Control Check) Periodic update. By default, this option is enabled. RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
- RRC Priority (1-8)—Specifies the priority bit set in the media stream. The priority can be any number between 1 and 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Choose an action from the drop-down list. The possible values are as follows:

  Drop—Specifies that a stream is dropped on periodic revaluation.

Fallback—Specifies that a stream is demoted to Best Effort class on periodic reevaluation.

The default value is **drop**.

h) Click **Apply**.

Step 3 Enable the media stream for multicast-direct by following these steps:

a) Choose **WLANs** > WLAN ID to open the WLANs > Edit page.
b) Click the **QoS** tab and select Gold (Video) from the Quality of Service (QoS) drop-down list.
c) Click **Apply**.

Step 4 Set the EDCA parameters to voice and video optimized (optional) by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **EDCA Parameters**.
b) From the **EDCA Profile** drop-down list, choose the Voice and Video Optimized option.
c) Click **Apply**.

Step 5 Enable the admission control on a band for video (optional) by following these steps:

Note Keep the voice bandwidth allocation to a minimum for better performance.

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a/n (5 GHZ) or 802.11b/g/n > Media page.
b) Click the **Video** tab.
c) Select the **Admission Control (ACM)** check box to enable bandwidth-based CAC for this radio band. The default value is disabled.
d) Click **Apply**.

Step 6 Configure the video bandwidth by following these steps:

Note The template bandwidth that is configured for a media stream should be more than the bandwidth for the source media stream.

Note The voice configuration is optional. Keep the voice bandwidth allocation to a minimum for better performance.

a) Disable all WMM WLANs.
b) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a/n/ac (5 GHZ) or 802.11b/g/n > Media page.
c) Click the **Video** tab.
d) Select the **Admission Control (ACM)** check box to enable the video CAC for this radio band. The default value is disabled.
e) In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.
f) The range is 5 to 85%.
g) The default value is 9%.
h) Click **Apply**.
i) Reenable all WMM WLANs and click **Apply**.

Step 7 Configure the media bandwidth by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a (or 802.11b) > Media > Parameters page.
b) Click the **Media** tab to open the Media page.
c) Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.

d) In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band.
e) The default value is 85%; valid values are from 0% to 85%.
f) In the **Client Minimum Phy Rate** text box, enter the minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
g) In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
h) Select the **Multicast Direct Enable** check box to enable the Multicast Direct Enable field. The default value is enabled.
i) From the **Max Streams per Radio** drop-down list, choose the maximum number of streams allowed per radio from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.
j) From the **Max Streams per Client** drop-down list, choose the maximum number of streams allowed per client from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.
k) Select the **Best Effort QoS Admission** check box to enable best-effort QoS admission.
l) Click **Apply**.

Step 8 Enable a WLAN by following these steps:
a) Choose **WLANS > WLAN ID**. The WLANs > Edit page appears.
b) Select the **Status** check box.
c) Click **Apply**.

Step 9 Enable the 802.11 a/n/ac or 802.11 b/g/n network by following these steps:
a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network**.
b) Select the **802.11a** or **802.11b/g Network Status** check box to enable the network status.
c) Click **Apply**.

Step 10 Verify that the clients are associated with the multicast groups and group IDs by following these steps:
a) Choose **Monitor > Clients**. The Clients page appears.
b) Check if the 802.11a/n/ac or 802.11b/g/n network clients have the associated access points.
c) Choose **Monitor > Multicast**. The Multicast Groups page appears.
d) Select the **MGID** check box for the VideoStream to the clients.
e) Click **MGID**. The Multicast Group Detail page appears. Check the Multicast Status details.

Configuring VideoStream (CLI)

Step 1 Configure the multicast-direct feature on WLANs media stream by entering this command:
config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Step 2 Enable or disable the multicast feature by entering this command:
config media-stream multicast-direct {**enable** | **disable**}

Step 3 Configure various message configuration parameters by entering this command:
config media-stream message {**state** [**enable** | **disable**] | **url** *url* | **email** *email* | **phone** *phone _number* | **note** *note*}

Step 4 Save your changes by entering this command:
save config

Step 5 Configure various global media-stream configurations by entering this command:
config media-stream add multicast-direct stream-name *media_stream_name start_IP end_IP* [**template** {**very-coarse** | **coarse** | **ordinary** | **low-resolution** | **med-resolution** | **high-resolution**} | **detail** {**Max_bandwidth** *bandwidth* | **packet size** *packet_size* | **Re-evaluation** *re-evaluation* {*periodic* | *initial*}} **video** *video* **priority** {**drop** | **fallback**}

- The Resource Reservation Control (RRC) parameters are assigned with the predefined values based on the values assigned to the template.
- The following templates are used to assign RRC parameters to the media stream:
  - Very Coarse (below 3000 kbps)
  - Coarse (below 500 kbps)
  - Ordinary (below 750 kbps)
  - Low Resolution (below 1 mbps)
  - Medium Resolution (below 3 mbps)
  - High Resolution (below 5 mbps)

Step 6 Delete a media stream by entering this command:
config media-stream delete *media_stream_name*

Step 7 Enable a specific enhanced distributed channel access (EDC) profile by entering this command:
config advanced{ **801.11a** | **802.11b**} **edca-parameters optimized-video-voice**

Step 8 Enable the admission control on the desired bandwidth by entering the following commands:

- Enable bandwidth-based voice CAC for 802.11a or 802.11b/g network by entering this command:

  config {**802.11a** | **802.11b**} **cac voice acm enable**

- Set the percentage of the maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:

  config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

- Configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network by entering this command:

  config {**802.11a** | **802.11b**} **cac voice roam-bandwidth** *bandwidth*

Note For TSpec and SIP based CAC for video calls, only Static method is supported.

Step 9 Set the maximum number of streams per radio and/or per client by entering these commands:

- Set the maximum limit to the number multicast streams per radio by entering this command:

config {**802.11a** | **802.11b**} **media-stream multicast-direct radio-maximum** [*value* | **no-limit**]

- Set the maximum number of multicast streams per client by entering this command:

  config {**802.11a** | **802.11b**} **media-stream multicast-direct client-maximum** [*value* | **no-limit**]

Step 10 Save your changes by entering this command:
save config

Viewing and Debugging Media Streams

- See the configured media streams by entering this command:

  show wlan *wlan_id*

- See the details of the media stream name by entering this command:

  show 802.11{a | b | h} media-stream *media-stream_name*

- See the clients for a media stream by entering this command:

  show 802.11a media-stream client *media-stream-name*

- See a summary of the media stream and client information by entering this command:

  show media-stream group summary

- See details about a particular media stream group by entering this command:

  show media-stream group detail *media_stream_name*

- See details of the 802.11a or 802.11b media resource reservation configuration by entering this command:

  show {802.11a | 802.11b} media-stream rrc

- Enable debugging of the media stream history by entering this command:

  debug media-stream history {enable | disable}

Configuring Multicast Domain Name System

Information About Multicast Domain Name System

Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the services on the local network. The mDNS service discovery enables wireless clients to access Apple services such as Apple Printer and Apple TV advertised in a different Layer 3 network. mDNS performs DNS queries over IP multicast. mDNS supports zero-configuration IP networking. As a standard, mDNS uses multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Location Specific Services

The processing of mDNS service advertisements and mDNS query packets support Location-Specific Services (LSS). All the valid mDNS service advertisements that are received by the controller are tagged with the MAC address of the AP that is associated with the service advertisement from the service provider while inserting the new entry into the service provider database. The response formulation to the client query filters the wireless entries in the SP-DB using the MAC address of the AP associated with the querying client. The wireless service provider database entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service. If LSS is disabled for any service, the wireless service provider database entries are not filtered when they respond to any query from a wireless client for the service.

LSS applies only to wireless service provider database entries. There is no location awareness for wired service provider devices.

The status of LSS cannot be enabled for services with ORIGIN set to wired and vice-versa.

mDNS AP

The mDNS AP feature allows the controller to have visibility of wired service providers that are on VLANs that are not visible to the controller. You can configure any AP as an mDNS AP and enable the AP to forward mDNS packets to the controller. VLAN visibility on the controller is achieved by APs that forward the mDNS advertisements to the controller. The mDNS packets between the AP and the controller are forwarded in Control and Provisioning of Wireless Access Points (CAPWAP) data tunnel that is similar to the mDNS packets from a wireless client. Only CAPWAPv4 tunnels are supported. APs can be in either the access port or the trunk port to learn the mDNS packets from the wired side and forward them to the controller.

You can use the configurable knob that is provided on the controller to start or stop mDNS packet forwarding from a specific AP. You can also use this configuration to specify the VLANs from which the AP should snoop the mDNS advertisements from the wired side. The maximum number of VLANs that an AP can snoop is 10.

If the AP is in the access port, you should not configure any VLANs on the AP to snoop. The AP sends untagged packets when a query is to be sent. When an mDNS advertisement is received by the mDNS AP, the VLAN information is not passed on to the controller. The service provider's VLAN that is learned through the mDNS AP's access VLAN is maintained as 0 in the controller.

By default, the mDNS AP snoops in native VLAN. When an mDNS AP is enabled, native VLAN snooping is enabled by default and the VLAN information is passed as 0 for advertisements received on the native VLAN.

The mDNS AP feature is supported only on local mode and monitor mode APs.

The mDNS AP configuration is retained on those mDNS APs even if global mDNs snooping is disabled.

Note There is no check to ensure that no two mDNS APs are duplicating the same traffic for the same service. But, for the same VLAN, there is such a check.

If an mDNS AP is reset or associated with the same controller or another controller, one of the following occurs:

- If the global snooping is disabled on the controller, a payload is sent to the AP to disable mDNS snooping.
- If the global snooping is enabled on the controller, the configuration of the AP before the reset or the association procedure is retained.

The process flow for the mDNS AP feature is as follows:

- Uplink (Wired infrastructure to AP to Controller):
  1. Receives the 802.3 mDNS packet on configured VLANs.
  2. Forwards the received mDNS packet over CAPWAP.
  3. Populates multicast group ID (MGID) based on the received VLAN.
- Downlink (Controller to AP to Wired Infrastructure):
  1. Receives an mDNS query over CAPWAP from the controller.
  2. Forwards the query as 802.3 packet to wired infrastructure.
  3. The VLAN is identified from dedicated MGIDs.

Per-Service SP Count Limit

The following list shows the global service provider limit per controller model:

- Cisco 8510 WLC—16000
- Cisco Flex 7510 WLC—16000
- Cisco 5508 WLC—6400
- Cisco 2504 WLC—6400

If the total number of service providers for all services is within the specified limit, any service is free to learn or discover as many other services. There is no per service reservation or restriction, which allows flexibility to accommodate more service providers for any service with respect to other services.

Priority MAC Support

You can configure up to 50 MAC addresses per service; these MAC addresses are the service provider MAC addresses that require priority. This guarantees that any service advertisements originating from these MAC addresses for the configured services are learned even if the service provider database is full by deleting the last nonpriority service provider from the service that has the highest number of service providers. When you configure the priority MAC address for a service, there is an optional parameter called ap-group, which is applicable only to wired service providers to associate a sense of location to the wired service provider devices. When a client mDNS query originates from this ap-group, the wired entries with priority MAC and ap-group are looked up and the wired entries are listed first in the aggregated response.

Origin-Based Service Discovery

You can configure a service to filter inbound traffic that is based on its origin, that is either wired or wireless. All the services that are learned from an mDNS AP are treated as wired. When the learn origin is wired, the LSS cannot be enabled for the service because LSS applies only to wireless services.

A service that has its origin set to wireless cannot be changed to wired if the LSS status is enabled for the service because LSS is applicable only to wireless service provider database. If you change the origin between wired and wireless, the service provider database entries with the prior origin type is cleared.

Restrictions for Configuring Multicast DNS

- mDNS over IPv6 is not supported.
- mDNS is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points.
- mDNS is not supported on remote LANs.
- mDNS is not supported on Cisco AP1240 and Cisco AP1130.
- Third-party mDNS servers or applications are not supported on the Cisco WLC using the mDNS feature. Devices that are advertised by the third-party servers or applications are not populated on the mDNS service or device table correctly on the Cisco WLC.
- In a Layer2 network, if Apple servers and clients are in the same subnet, mDNS snooping is not required on the Cisco WLC. However, this relies on the switching network to work. If you use switches that do not work as expected with mDNS snooping, you must enable mDNS on the Cisco WLC.
- Video is not supported on Apple iOS 6 with WMM in enabled state.
- mDNS APs cannot duplicate the same traffic for the same service or VLAN.
- LSS filtering is restricted to only wireless services.
- The LSS, mDNS AP, Priority MAC address, and origin-based discovery features cannot be configured using the controller GUI.
- mDNS-AP feature is not supported in CAPWAP V6.
- ISE dynamic mDNS policy mobility is not supported.
- mDNS user profile mobility is not supported in guest anchors.
- Mobility: ISE dynamic mDNS policy creation in foreign controllers is inconsistent.
- Apple devices such as iPads and iPhones can discover Apple TV through Bluetooth. This might result in Apple TVs being visible to end users. Because Apple TVs are not supported on mDNS access policy, we recommend that you disable Bluetooth on Apple TVs.

Configuring Multicast DNS (GUI)

Step 1 Configure the global mDNS parameters and the Master Services Database by following these steps:

a) Choose **Controller** > **mDNS** > **General**.
b) Select or unselect the **mDNS Global Snooping** check box to enable or disable snooping of mDNS packets, respectively.
c) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service.
d) Choose a service from the **Select Service** drop-down list.

Note To add a new mDNS-supported service to the list, choose **Other**. Specify the service name and the service string. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services Database. The controller can snoop and learn a maximum of 64 services.

e) Select or unselect the **Query Status** check box to enable or disable an mDNS query for a service, respectively.
f) Click **Add**.
g) Click **Apply**.
h) To view the details of an mDNS service, hover your cursor over the blue drop-down arrow of a service, and choose **Details**.

Step 2 Configure an mDNS profile by following these steps:

a) Choose **Controller** > **mDNS** > **Profiles**.
The controller has a default mDNS profile, which is default-mdns-profile. It is not possible to delete the default profile.

b) To create a new profile, click **New**, enter a profile name, and click **Apply**.
c) To edit a profile, click a profile name on the **mDNS Profiles** page; from the **Service Name** drop-down list, choose a service to be associated with the profile, and click **Apply**.
You can add multiple services to a profile.

Step 3 Click **Save Configuration**.

What to Do Next

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The highest priority is given to the profiles associated with interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

- Map an mDNS profile to an interface group by following these steps:
  1. Choose **Controller** > **Interface Groups**.
  2. Click the corresponding interface group name.
     The **Interface Groups > Edit** page is displayed.
  3. From the **mDNS Profile** drop-down list, choose a profile.
- Map an mDNS profile to an interface by following these steps:
  1. Choose **Controller** > **Interfaces**.
  2. Click the corresponding interface name.
     The **Interfaces > Edit** page is displayed.
  3. From the **mDNS Profile** drop-down list, choose a profile.
- Map an mDNS profile to a WLAN by following these steps:
  1. Choose **WLANs**. click the WLAN ID to open the WLANs > Edit page.
  2. Click the corresponding WLAN ID.
     The **WLANs > Edit** page is displayed.
  3. Click the **Advanced** tab.
  4. Select the **mDNS Snooping** check box.

5 From the **mDNS Profile** drop-down list, choose a profile.

Note The wireless controller advertises the services from the wired devices (such as Apple TVs) learnt over VLANs, when:

- mDNS snooping is enabled in the WLAN Advanced options.
- mDNS profile is enabled either at interface group (if available), interface, or WLAN.

Configuring Multicast DNS (CLI)

- Configure mDNS snooping by entering this command:

  config mdns snooping {**enable** | **disable**}

- Configure mDNS services by entering this command:

  config mdns service {{**create** *service-name service-string* **origin** {**wireless** | **wired** | **all**} **lss** {**enable** | **disable**} [**query**] [**enable** | **disable**]} | **delete** *service-name*}

- Configure a query for an mDNS service by entering this command:

  config mdns service query {**enable** | **disable**} *service-name*

- Configure a query interval for mDNS services by entering this command:

  config mdns query interval *value-in-minutes*

- Configure an mDNS profile by entering this command:

  config mdns profile {**create** | **delete**} *profile-name*

  Note If you try to delete an mDNS profile that is already associated with an interface group, an interface, or a WLAN, an error message is displayed.

- Configure mDNS services to a profile by entering this command:

  config mdns profile service {**add** | **delete**} *profile-name service-name*

- Map an mDNS profile to an interface group by entering this command:

  config interface group mdns-profile {*interface-group-name* | **all**} {*mdns-profile-name* | **none**}

  Note If the mDNS profile name is **none**, no profiles are attached to the interface group. Any existing profile that is attached is removed.

- View information about an mDNS profile that is associated with an interface group by entering this command:

  show interface group detailed *interface-group-name*

- Map an mDNS profile to an interface by entering this command:
  config interface mdns-profile {**management** | {*interface-name* | **all**}} {*mdns-profile-name* | **none**}
- View information about the mDNS profile that is associated with an interface by entering this command:
  show interface detailed *interface-name*
- Configure mDNS for a WLAN by entering this command:
  config wlan mdns {**enable** | **disable**} {*wlan-id* | **all**}
- Map an mDNS profile to a WLAN by entering this command:
  config wlan mdns profile {*wlan-id* | **all**} {*mdns-profile-name* | **none**}
- View information about an mDNS profile that is associated with a WLAN by entering this command:
  show wlan *wlan-id*
- View information about all mDNS profiles or a particular mDNS profile by entering this command:
  show mdns profile {**summary** | **detailed** *mdns-profile-name*}
- View information about all mDNS services or a particular mDNS service by entering this command:
  show mdns service {**summary** | **detailed** *mdns-service-name*}
- View information about the mDNS domain names that are learned by entering this command:
  show mdns domain-name-ip summary
- View the mDNS profile for a client by entering this command:
  show client detail *client-mac-address*
- View the mDNS details for a network by entering this command:
  show network summary
- Clear the mDNS service database by entering this command:
  clear mdns service-database {**all** | *service-name*}
- View events related to mDNS by entering this command:
  debug mdns message {**enable** | **disable**}
- View mDNS details of the events by entering this command:
  debug mdns detail {**enable** | **disable**}
- View errors related to mDNS processing by entering this command:
  debug mdns error {**enable** | **disable**}
- Configure debugging of all mDNS details by entering this command:
  debug mdns all {**enable** | **disable**}
- Location Specific Service-related commands:
  - Enable or disable location specific service on a specific mDNS service or all mDNS services by entering this command:
    config mdns service lss {**enable** | **disable**} {*service-name* | **all**}

Note By default, LSS is in disabled state.

Impact on High Availability: Requires to be synchronized with the standby controller.

- View the status of LSS by entering these commands:
  Summary—**show mdns service summary**

  Detailed—**show mdns service detailed** *service-name*
- Configure troubleshooting HA-related mDNS by entering this command:
  debug mdns ha {**enable** | **disable**}

• Origin-based service discovery-related commands:

- Configure learning of services from wired, wireless, or both by entering this command:
  config mdns service origin {**Wireless** | **Wired** | **All**} {*service-name* | **all**}

  It is not possible to configure wired services if LSS is enabled and vice versa. It is not possible to enable LSS for wired-only service learn origin.

  Impact on High Availability: Requires to be synchronized with the standby controller.
- View the status of origin-based service discovery by entering this command:
  Summary—**show mdns service summary**

  Detailed—**show mdns service detailed** *service-name*
- View all the service advertisements that are present in the controller, but not discovered because of restrictions on learning those services, by entering this command:
  show mdns service not-learnt

  Service advertisements across all VLANs and origin types that are not learned are displayed.

• Priority MAC address-related commands:

- Configure per-service MAC addresses of service-providing devices to ensure that they are snooped and discovered even if the service provider database is full, by entering this command:
  config mdns service priority-mac {**add** | **delete**} *priority-mac-addr service-name* **ap-group** *ap-group-name*

  The optional AP group is applicable only to wired service provider devices to give them a sense of location; these service providers are placed higher in the order than the other wired devices.
- View the status of Priority MAC address by entering this command:
  Detailed—**show mdns service detailed** *service-name*

• mDNS AP-related commands:

- Enable or disable mDNS forwarding on an AP that is associated with the controller by entering this command:
  config mdns ap {**enable** | **disable**} {*ap-name* | **all**} **vlan** *vlan-id*

  There is no default mDNS AP. VLAN ID is an optional node.

  Impact on High Availability: The static configuration is synchronized to the standby controller.

- Configure the VLAN on which the AP should snoop, and forward the mDNS packets by entering this command:
  config mdns ap vlan {**add** | **delete**} *vlan-id ap-name*
- View all the APs for which mDNS forwarding is enabled by entering this command:
  show mdns ap summary

Information about Bonjour gateway based on access policy

From 7.4 release WLC supports Bonjour gateway functionality on WLC itself for which you need not even enable multicast on the controller. The WLC explores all Bonjour discovery packets and does not forward them on AIR or Infra network.

Bonjour is Apple's version of Zeroconf - it is Multicast Domain Name System (mDNS) with DNS-SD (Domain Name System-Service Discovery). Apple devices will advertise their services via IPv4 and IPv6 simultaneously (IPv6 link local and Globally Unique). To address this issue Cisco WLC acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc) from the source/host e.g. AppleTV and responds to Bonjour clients when they ask/request for a service.

Bonjour gateway has inadequate capabilities to filter cached wired or wireless service instances based on the credentials of the querying client and its location.

Currently the limitations are:

- Location-Specific Services (LSS) filters the wireless service instances only while responding to a query from wireless clients. The filtering is based on the radio neighborhood of the querying client.
- LSS cannot filter wired service instance because of no sense of location.
- LSS filtering is per service type and not per client. It means that all clients receive the location based filtered response if LSS is enabled for the service type and clients cannot override the behavior.
- There is no other filtering mechanism based on client role or user-id.

The requirement is to have configuration per service instance.

Following are the three criteria of the service instance sharing:

- User-id
- Client-role
- Client location

The configuration can be applied to wired and wireless service instances. The response to any query is on the policy configured for each service instance. The response enables the selective sharing of service instances based on the location, user-id or role.

As the most service publishing devices are wired, the configuration allows filtering of wired services at par with the wireless service instances.

There are two levels of filtering client queries:

1. At the service type level by using the mDNS profile
2. At the service instance level using the access policy associated with the service.

Restrictions to the Bonjour gateway based on access policy

- The total number of policies that can be created is same as the number of service instances that are supported on the platform. Hundred policies can be supported; 99 policies and one default policy.
- The number of rules per policy is limited to one.
- Policy and rules can be created irrespective of the service instances. The policy is applied only when it is complete and discovers the target service instances.
- A service instance can be associated with a maximum of five policies.
- Five service groups can be assigned for a MAC address.

Creating Bonjour Access Policy through Prime Infrastructure

The admin user can create the Bonjour access policy using the GUI of the Prime Infrastructure (PI).

Step 1 Log in to the Cisco Prime Infrastructure using the Admin credentials.

Step 2 Choose **Administration** > **AAA** > **Users** > **Add User**.

Step 3 Choose **mDNS Policy Admin**.

Step 4 Add or remove the devices in the mDNS Device Filter. Click **Save**.

Step 5 Add the users for a device in the Users list dialog box. Click **Save**.

Note See Cisco Prime Infrastructure Administrator Guide for the release 2.2 for more details.

Configuring mDNS Service Groups (GUI)

Step 1 Choose **Controller** > **mDNS** > **mDNS Policies**.

Step 2 Select service group from the list of Group Names.

Step 3 Under Service Instance List perform the following steps:

a) Enter the service provider MAC address in MAC address.

b) Enter the name of service provider in **Name**. Click **Add**.

c) From the **Location Type** drop-down list, choose the type of location.

Note If the location is selected as 'Any', the policy checks on the location attribute are not performed.

In the case of mDNS policy filtered by AP groups, the design is for substring match. The policy is applied on the first substring match.

Note The list of current service instances associated with the service group is shown in a table.

Step 4 Under **Policy / Rule** enter the role names and the user names as the criteria of enforcing the policy.

Configuring mDNS Service Groups (CLI)

Step 1 Enable or disable the mDNS policy by entering this command: **config mdns policy enable | disable**

Step 2 Create or delete a mDNS policy service group by entering this command: **config mdns policy service-group create | delete** <*service-group-name*>

Step 3 Configure the parameters of a service group by entering this command: **config mdns policy service-group device-mac add** <*service-group-name*> <*mac-addr*> <*device name*> **location-type** *[<AP_LOCATION | AP_NAME | AP_GROUP>]* **device-location** *[<location string | any | same>]*

Step 4 Configure the user role for a service-group by entering this command: **config mdns policy service-group user-role add | delete** <*service-group-name*> <*user-role-name*>

Step 5 Configure the user name for a service-group by entering this command: **config mdns policy service-group user-name add | delete** <*service-group-name*> <*user-name*>