Configuring Multicast

- Configuring Multicast Mode, page 1
- Configuring Multicast Domain Name System, page 8
- Multicast Configuration for Cisco vWLC, Flex 7510, 5520, 8510, and 8540 WLCs, page 14

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.
When you disable the Global Multicast Mode, the controller still forwards the IPv6 ICMP multicast messages, such as router announcements and DHCPv6 solicit, 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 sends 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.

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.
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 Unified 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 controller, you also must configure a CAPWAP multicast group address. Access points subscribe to the CAPWAP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3.
- 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.
- Lightweight Access Points 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 2500 Series WLC, you have to configure the multicast IP address.

- Multicast mode is not supported on Cisco Flex 7500 Series WLCs.

- 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 platform'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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Global Multicast</th>
<th>Multicast Mode</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 5520, 8510, and 8540 WLCs</td>
<td>Enabled</td>
<td>Unicast</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td>Multicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Multicast</td>
<td>No</td>
</tr>
<tr>
<td>Cisco Flex 7510 WLC</td>
<td>Multicast is not supported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco 5508 WLC</td>
<td>Enabled</td>
<td>Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td>Multicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Multicast</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 2504 WLC</td>
<td>Only multicast mode is supported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco vWLC</td>
<td>Multicast is not supported</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 \( \text{timeout} / 3 \) 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 | disable {all | interface-name}}
```

**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
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
```

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.

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.

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 an mDNS service by entering this command:
  ```
  config mdns service {
  {create service-name service-string 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:
Configuring Multicast DNS (CLI)

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}

### 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).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Cisco Prime Infrastructure using the Admin credentials.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Administration &gt; AAA &gt; Users &gt; Add User.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose mDNS Policy Admin.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Add or remove the devices in the mDNS Device Filter. Click Save.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Add the users for a device in the Users list dialog box. Click Save.</td>
</tr>
</tbody>
</table>

**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>
```

---

**Multicast Configuration for Cisco vWLC, Flex 7510, 5520, 8510, and 8540 WLCs**

**Switching from Multicast-Unicast Mode to Multicast-Multicast Mode**

**Step 1**  
Assign both IPv4 and IPv6 (required only if IPv6 is enabled) multicast addresses by entering this command:  
a)  
```
config network multicast mode multicast IPv4-multicast-address
```
b)  
```
config ipv6 multicast mode multicast IPv6-multicast-address
```

**Step 2**  
Enable global multicast by entering this command:  
```
config network multicast global enable
```
Switching from Multicast-Multicast Mode to Multicast-Unicast Mode

Step 1
Disable global multicast by entering this command:
```
config network multicast global disable
```

Step 2
Configure the Multicast-Unicast mode by entering this command (IPv6 configuration is required only when IPv6 is enabled):

a) `config network multicast mode unicast`
b) `config ipv6 multicast mode unicast`

Restrictions

- We recommend that you do not switch from Multicast-Multicast mode to Multicast-Unicast mode on a loaded network because it can burden the network. We recommend that you use Multicast-Multicast mode on these platforms because of the scale factor.
- IGMP and MLD snooping cannot be enabled unless global multicast is enabled, and multicast mode is Multicast-Multicast.
- Global multicast can be enabled only when Multicast-Multicast mode is configured.
- Switching from Multicast-Multicast mode to Multicast-Unicast mode is not allowed if the global multicast is enabled. You must disable global multicast before switching the mode in this case.
- FlexConnect APs:
  - Can join in Multicast-Multicast mode from Release 8.0 onwards.
  - Multicast-Unicast mode has to be enabled if IPv6 support is required on FlexConnect APs by the central-switching clients. Therefore, IGMP or MLD snooping is not supported.
  - VideoStream is not supported because it requires IGMP or MLD snooping.

Troubleshooting

Unable to switch to Multicast-Multicast mode as Global Multicast is not getting enabled

Possible issue—IPv6 is configured but not in use. Check if IPv6 is still in Multicast-Unicast mode.

Solution—Disable IPv6 if it is not being used or switch Multicast-Unicast to Multicast-Multicast mode for IPv6.