WLAN Interfaces

- Multicast VLAN, on page 1
- Passive Clients, on page 2
- Dynamic Anchoring for Clients with Static IP Addresses, on page 7

Multicast VLAN

Information About Multicast Optimization

Prior to the 7.0.116.0 release, multicast was based on the grouping of the multicast address and the VLAN as one entity, MGID. With VLAN select and VLAN pooling, there is a possibility that you might increase duplicate packets. With the VLAN select feature, every client listens to the multicast stream on a different VLAN. As a result, the controller creates different MGIDs for each multicast address and VLAN. Therefore, the upstream router sends one copy for each VLAN, which results, in the worst case, in as many copies as there are VLANs in the pool. Since the WLAN is still the same for all clients, multiple copies of the multicast packet are sent over the air. To suppress the duplication of a multicast stream on the wireless medium and between the controller and access points, you can use the multicast optimization feature.

Multicast optimization enables you to create a multicast VLAN which you can use for multicast traffic. You can configure one of the VLANs of the WLAN as a multicast VLAN where multicast groups are registered. Clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using multicast VLAN and multicast IP addresses. If multiple clients on the VLAN pool of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The controller makes sure that all multicast streams from the clients on this VLAN pool always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN pool. Only one multicast stream hits the VLAN pool even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the air is just one stream.

Configuring a Multicast VLAN (GUI)

Procedure

Step 1
Choose WLANs > WLAN ID. The WLAN > Edit page appears.

Step 2
In the General tab, select the Multicast VLAN feature check box to enable multicast VLAN for the WLAN.
The Multicast Interface drop-down list appears.

**Step 3** Choose the VLAN from the Multicast Interface drop-down list.

**Step 4** Click **Apply**.

---

**Configuring a Multicast VLAN (CLI)**

Use the `config wlan multicast interface wlan_id enable interface_name` command to configure the multicast VLAN feature.

---

**Passive Clients**

### Information About Passive Clients

Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.

Wireless LAN controllers currently act as a proxy for ARP requests. Upon receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This scenario has two advantages:

- The upstream device that sends out the ARP request to the client will not know where the client is located.
- Power for battery-operated devices such as mobile phones and printers is preserved because they do not have to respond to every ARP requests.

Since the wireless controller does not have any IP related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Any application that tries to access a passive client will fail.

The passive client feature enables the ARP requests and responses to be exchanged between wired and wireless clients. This feature when enabled, allows the controller to pass ARP requests from wired to wireless clients until the desired wireless client gets to the RUN state.

**Note**

For FlexConnect APs with locally switched WLANs, passive client feature enables the broadcast of ARP requests and the APs respond on behalf of the client.

---

**Restrictions for Passive Clients**

- The interface associated to the WLAN must have a VLAN tagging.
- GARP forwarding must to be enabled using the `show advanced hotspot` command.
Client ARP forwarding will not work if any one of the two scenarios, mentioned above, is not configured.

- The passive client feature is not supported with the AP groups and FlexConnect centrally switched WLANs.

### Configuring Passive Clients (GUI)

**Before you begin**

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

**Procedure**

1. Choose **Controller > General** to open the General page.
2. From the **AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.
3. In the **Multicast Group Address** text box, enter the IP address of the multicast group.
4. Click **Apply**.
5. Enable global multicast mode as follows:
   a. Choose **Controller > Multicast**.
   b. Check the **Enable Global Multicast Mode** check box.

### Enabling the Multicast-Multicast Mode (GUI)

**Before you begin**

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

**Procedure**

1. Choose **Controller > General** to open the General page.
2. Choose one of the following options from the **AP Multicast Mode** drop-down list:
   - **Unicast**—Configures the controller to use the unicast method to send multicast packets. This is the default value.
   - **Multicast**—Configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.
3. From the **AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.
Step 4  In the **Multicast Group Address** text box, enter the IP address of the multicast group.

Step 5  Click **Apply**.

Step 6  Enable global multicast mode as follows:
   a)  Choose **Controller > Multicast**.
   b)  Check the **Enable Global Multicast Mode** check box.

---

### Enabling the Global Multicast Mode on Controllers (GUI)

**Procedure**

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

**Note**  The Enable IGMP Snooping text box is highlighted only when you enable the Enable Global Multicast mode. The IGMP Timeout (seconds) text box is highlighted only when you enable the Enable IGMP Snooping text box.

**Step 2**  Select the **Enable Global Multicast Mode** check box to enable the multicast mode. This step configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

**Step 3**  Select the **Enable IGMP Snooping** check box to enable the IGMP snooping. The default value is disabled.

**Step 4**  In the IGMP Timeout text box to set the IGMP timeout, enter a value between 30 and 7200 seconds.

**Step 5**  Click **Apply** to commit your changes.

---

### Enabling the Passive Client Feature on the Controller (GUI)

**Procedure**

**Step 1**  Choose **WLANs > WLANs > WLAN ID** to open the WLANs > Edit page. By default, the General tab is displayed.

**Step 2**  Choose the **Advanced** tab.

**Step 3**  Select the **Passive Client** check box to enable the passive client feature.

**Step 4**  Click **Apply** to commit your changes.

---

### Configuring Passive Clients (CLI)

**Procedure**

**Step 1**  Enable multicasting on the controller by entering this command:

```bash
config network multicast global enable
```
The default value is disabled.

**Step 2**
Configure the controller to use multicast to send multicast to an access point by entering this command:

```
config network multicast mode multicast multicast_group_IP_address
```

**Step 3**
Configure passive client on a wireless LAN by entering this command:

```
config wlan passive-client {enable | disable} wlan_id
```

**Step 4**
Configure a WLAN by entering this command:

```
config wlan
```

**Step 5**
Save your changes by entering this command:

```
save config
```

**Step 6**
Display the passive client information on a particular WLAN by entering this command:

```
show wlan 2
```

**Step 7**
Verify if the passive client is associated correctly with the AP and if the passive client has moved into the DHCP required state at the controller by entering this command:

```
debug client mac_address
```

**Step 8**
Display the detailed information for a client by entering this command:

```
show client detail mac_address
```

**Step 9**
Check if the client moves into the run state, when a wired client tries to contact the client by entering this command:

```
debug client mac_address
```

**Step 10**
Configure and check if the ARP request is forwarded from the wired side to the wireless side by entering this command:

```
debug arp all enable
```

**Note**
Cisco WLC detects duplicate IP addresses based on the ARP table, and not based on the VLAN information. If two clients in different VLANs are using the same IP address, Cisco WLC reports IP conflict and sends GARP. This is not limited to two wired clients, but also for a wired client and a wireless client.

---

**Information About Multicast-to-Unicast Support for Passive Client ARPs**

This feature is designed to function on the Cisco 5520 WLC. After the passive client feature is enabled on the Cisco WLC, it accommodates non-Cisco WGBs so that all the traffic gets routed from the wired clients through the WGB and to the APs.

In this implementation, the broadcast ARP messages are sent to all the APs. When the Multicast-to-unicast mode is enabled on the Cisco 5520 WLC, the traffic is sent to the APs as Unicast packets using this mode.
Restrictions in Multicast-to-Unicast Support for Passive Client ARPs

- Supported on 5520 WLC only.
- A limitation of 10,000 packets per second is applied to avoid high CPU utilization.
- The passive client feature is supported on per WLAN basis.

Configuring Unicast mode on WLC (GUI)

**Procedure**

1. Choose WLANs to open the WLANs page
2. Click the ID number of the WLAN for which you want to configure the passive-client unicast mode.
3. Choose **Advanced** tab.
4. Check the **Passive Client** check box.
5. Click **Apply** to save your configuration.
6. Choose **Controller** page
7. From the ARP Unicast Mode drop-down list, choose **enable**.
8. Click **Apply** to save your configuration.

Configuring Unicast mode on WLC (CLI)

**Procedure**

1. Enable passive client before enabling Unicast mode.
   
   `config wlan passive-client enable wlan-id`

2. Enable Unicast packet forwarding.
   
   `config network passive-client arp-unicast-forwarding enable`

3. View the status of ARP Unicast mode
   
   `show network summary`

4. View the ARP statistics
   
   `show arp stats`

5. View the status of passive client
   
   `show wlan wlan-id`
Dynamic Anchoring for Clients with Static IP Addresses

Information About Dynamic Anchoring for Clients with Static IP

At times you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses.

Dynamic anchoring of static IP clients with static IP addresses can be associated with other controllers where the client’s subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.

How Dynamic Anchoring of Static IP Clients Works

The following sequence of steps occur when a client with a static IP address tries to associate with a controller:

1. When a client associates with a controller, for example, WLC-1, it performs a mobility announcement. If a controller in the mobility group responds (for example WLC-2), the client traffic is tunneled to the controller WLC-2. As a result, the controller WLC 1 becomes the foreign controller and WLC-2 becomes the anchor controller.

2. If none of the controllers responds, the client is treated as a local client and authentication is performed. The IP address for the client is updated either through an orphan packet handling or an ARP request processing. If the IP subnet of the client is not supported in the controller (WLC-1), WLC-1 sends another static IP mobile announce and if a controller (for example WLC-3) that supports the client's subnet responds to that announcement, the client traffic is tunneled to that controller, that is WLC-3. As a result, the controller WLC 1 becomes the export foreign controller and WLC-3 becomes the export anchor controller.

3. Once the acknowledgment is received, the client traffic is tunneled between the anchor and the controller (WLC-1).

Note

If you configure WLAN with an interface group and any of the interfaces in the interface group supports the static IP client subnet, the client is assigned to that interface. This situation occurs in local or remote (static IP Anchor) controller.

When AAA override is used along with the interface group that is mapped to WLAN, the source interface that is used for DHCP transactions is the Management interface.

If the interface group that you add to a WLAN has RADIUS Server Overwrite interface enabled and a client requests for authentication, the controller selects the first IP address from the interface group as the RADIUS server.

Note

A security level 2 authentication is performed only in the local (static IP foreign) controller, which is also known as the exported foreign controller.
Restrictions on Dynamic Anchoring for Clients With Static IP Addresses

- Do not configure overridden interfaces when you perform AAA for static IP tunneling, this is because traffic can get blocked for the client if the overridden interface does not support the client’s subnet. This can be possible in extreme cases where the overriding interface group supports the client’s subnet.
- The local controller must be configured with the correct AAA server where this client entry is present.

The following restrictions apply when configuring static IP tunneling with other features on the same WLAN:

- Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN.
- FlexConnect local authentication cannot be configured for the same WLAN.
- The DHCP required option cannot be configured for the same WLAN.
- You cannot configure dynamic anchoring of static IP clients with FlexConnect local switching.
- We recommend that you configure the same NTP/SNTP servers on the Cisco WLCs. If the NTP/SNTP servers are different, ensure that the system time on all Cisco WLCs is the same when NTP/SNTP is enabled. If the system time is not in sync, seamless mobility might fail in some scenarios. Also, a Cisco WLC that has the lagging time with NTP/SNTP enabled drops the mobile announce messages.

Configuring Dynamic Anchoring of Static IP Clients (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose WLANs to open the WLANs page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the ID number of the WLAN on which you want to enable dynamic anchoring of IP clients. The WLANs &gt; Edit page is displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the Advanced tab to open the WLANs &gt; Edit (Advanced) page.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enable dynamic anchoring of static IP clients by selecting the Static IP Tunneling check box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Apply to commit your changes.</td>
</tr>
</tbody>
</table>

**Configuring Dynamic Anchoring of Static IP Clients (CLI)**

`config wlan static-ip tunneling {enable | disable} wlan_id`— Enables or disables the dynamic anchoring of static IP clients on a given WLAN.

To monitor and troubleshoot your controller for clients with static IP, use the following commands:

- `show wlan wlan_id`—Enables you to see the status of the static IP clients feature.

```
Static IP client tunneling............... Enabled
```

- `debug client client-mac`
• debug dot11 mobile enable
• debug mobility handoff enable