Configuring Passive Clients

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.

Note 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.
- If ARP caching is enabled, APs reply to ARP requests on behalf of clients in locally-switched WLANs. If you have enabled passive clients for a WLAN and if an ARP request is received for an unknown client, the ARP packet is broadcast to all clients connected to the WLAN. However, if you have enabled AAA override for the WLAN, the ARP request for the unknown client is dropped by the AP because the AP does not have a mapping between the VLAN in which the ARP request is made and the WLAN to which the client is connected.

  Without WLAN-VLAN mapping, APs cannot find the corresponding WLAN for the VLAN of incoming ARP requests. Therefore, the APs cannot check if passive clients are enabled for the WLAN.

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.

This section contains the following subsections:

Configuring Passive Clients (GUI)

Before you begin

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

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

Step 2 From **the AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.

Step 3 In the **Multicast Group Address** text box, enter the IP address of the multicast group.

Step 4 Click **Apply**.

Step 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.

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

Step 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.

Step 3 From the **AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.

Note It is not possible to configure the AP multicast mode for Cisco Flex 7510 WLCs because only unicast is supported.

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)

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.

Note It is not possible to configure Global Multicast Mode for Cisco Flex 7510 WLCs.

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)

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)

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

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 Controller 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.

Configuring the Gratuitous ARP (GARP) Forwarding to Wireless Networks

Procedure

- To configure the gratuitous ARP (GARP) forwarding to wireless networks, enter this command:

  config advanced hotspot garp {**enable** | **disable**}