Client Traffic Forwarding Configurations

802.3 Bridging

The controller supports 802.3 frames and the applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

You can also configure 802.3 bridging using the Cisco Prime Network Control System. See the *Cisco Prime Network Control System Configuration Guide* for instructions.

This section contains the following subsections:

Restrictions on 802.3 Bridging

- Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP.

  The raw 802.3 frame contains destination MAC address, source MAC address, total packet length, and payload.

- By default, Cisco WLCs bridge all non-IPv4 packets (such as AppleTalk, IPv6, and so on). You can also use ACLs to block the bridging of these protocols.

Configuring 802.3 Bridging (GUI)

Procedure

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

Step 2 From the **802.3 Bridging** drop-down list, choose **Enabled** to enable 802.3 bridging on your controller or **Disabled** to disable this feature. The default value is Disabled.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring 802.3 Bridging (CLI)

Procedure

Step 1 See the current status of 802.3 bridging for all WLANs by entering this command:

show network

Step 2 Enable or disable 802.3 bridging globally on all WLANs by entering this command:

config network 802.3-bridging {**enable** | **disable**}

The default value is disabled.

Step 3 Save your changes by entering this command:

save config

Enabling 802.3X Flow Control

802.3X Flow Control is disabled by default. To enable it, enter the **config switchconfig flowcontrol enable** command.

Bridging Link Local Traffic

This section contains the following subsections:

Configuring Bridging of Link Local Traffic (GUI)

Configure bridging of link local traffic at the local site by following these steps:

Procedure

Step 1 Choose **Controller** > **General**.

Step 2 From the **Link Local Bridging** drop-down list, choose **Enabled** or **Disabled**.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Bridging of Link Local Traffic (CLI)

Procedure

- Configure bridging of link local traffic at the local site by using this command:

  config network link-local-bridging {**enable** | **disable**}

IP-MAC Address Binding

The controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. The controller checks only the MAC address of the client and ignores the IP address. Disable IP-MAC Address Binding if you have a wireless client that has multiple IP addresses mapped to the same MAC address. Examples include a PC running a VM software in Bridge mode, or a third-party WGB.

You must disable IP-MAC address binding to use an access point in sniffer mode if the access point is associated with a Cisco 2504 Wireless Controller, a Cisco 5508 Wireless Controller, or a controller network module. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable**.

WLAN must be enabled to use an access point in sniffer mode if the access point is associated with a Cisco 2504 Wireless Controller, a Cisco 5508 Wireless Controller, or a controller network module. If WLAN is disabled, the access point cannot send packets.

Note If the IP address or MAC address of the packet has been spoofed, the check does not pass, and the controller discards the packet. Spoofed packets can pass through the controller only if both the IP and MAC addresses are spoofed together and changed to that of another valid client on the same controller.

This section contains the following subsection:

Configuring IP-MAC Address Binding (CLI)

Procedure

Step 1 Enable or disable IP-MAC address binding by entering this command:

config network ip-mac-binding {**enable** | **disable**}

The default value is enabled.

Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

Note You must disable this binding check in order to use an access point in sniffer mode if the access point is joined to a Cisco 5508 WLC.

Step 2 Save your changes by entering this command:

save config

Step 3 View the status of IP-MAC address binding by entering this command:

show network summary

Information similar to the following appears:

```
RF-Network Name............................. ctrl4404
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
...

IP/MAC Addr Binding Check ............... Enabled

...<?Line-Break?><?HardReturn?>
```

TCP Adjust MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem, you can specify the MSS for all access points that are joined to the controller or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

In Release 8.5 and later releases, TCP Adjust MSS is enabled by default with a value of 1250. We recommend that you do not change this default value.

Note The previously configured TCP Adjust MSS settings are carried forward when you upgrade the controller software. The default TCP Adjust MSS values are applied to new controller configurations only.

TCP Adjust MSS is supported only on APs that are in local mode or FlexConnect with centrally switched WLANs.

This section contains the following subsections:

Configuring TCP Adjust MSS (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Under **TCP MSS**, check the **Global TCP Adjust MSS** check box and set the MSS for all APs that are associated with the controller.

The valid ranges are:

- For IPv4, TCP must be between 536 and 1363 bytes.
- For IPv6, TCP must be between 1220 and 1331 bytes.

Note Any TCP Adjust MSS value that is below 1220 and above 1331 will not be effective for CAPWAPv6 AP. The recommended value is 1250.

Configuring TCP Adjust MSS (CLI)

Procedure

Step 1 Enable or disable the TCP Adjust MSS on a particular access point or on all access points by entering this command:

config ap tcp-mss-adjust {**enable** | **disable**} {*Cisco_AP* | *all*} *size*

where the *size* parameter is a value between 536 and 1363 bytes for IPv4 and between 1220 and 1331 for IPv6. The default value varies for different clients.

The valid ranges are:

- For IPv4, TCP must be between 536 and 1363 bytes.
- For IPv6, TCP must be between 1220 and 1331 bytes.

Note Any TCP Adjust MSS value that is below 1220 and above 1331 will not be effective for CAPWAPv6 AP. The recommended value is 1250.

Step 2 Save your changes by entering this command:

save config

Step 3 See the current TCP Adjust MSS setting for a particular access point or all access points by entering this command:

show ap tcp-mss-adjust {*Cisco_AP* | **all**}

Information similar to the following appears:

```
AP Name             TCP State  MSS Size
```

```
------------------   --------   -------
AP58AC.78DC.A810     disabled   -
APa89d.21b2.2688     enabled    1250
AP00FE.C82D.DE80     disabled   -
```

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:

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.

Configuring Passive Clients (GUI)

Before you begin

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

Procedure

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.

Configuring Passive Clients (CLI)

Procedure

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**}

Enabling the Multicast-Multicast Mode (GUI)

Before you begin

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

Procedure

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)

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.

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)

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.