Global Traffic Forwarding Configurations

Configuring IPv6 Neighbor Discovery Caching

Information About IPv6 Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

At any given time, only eight IPv6 addresses are supported per client. When the ninth IPv6 address is encountered, the controller removes the oldest stale entry and accommodates the latest one.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the controller track each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

Configuring Neighbor Binding (GUI)

Step 1 Choose **Controller > IPv6 > Neighbor Binding** page.

Step 2 Configure the following:

- Down–Lifetime—Specifies how long IPv6 cache entries are kept if the interface goes down. The range is from 0 to 86400 seconds.
- Reachable–Lifetime—Specifies how long IPv6 addresses are active. The range is from 0 to 86400 seconds.

• Stale–Lifetime—Specifies how long to keep IPv6 addresses in the cache. The range is from 0 to 86400 seconds.

Step 3 Enable or disable the Unknown Address Multicast NS Forwarding.

Step 4 Enable or disable NA Multicast Forwarding.
If you enable NA Multicast Forwarding, all unsolicited multicast NA from Wired/Wireless is not forwarded to Wireless.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Neighbor Binding (CLI)

- Configure the neighbor binding parameters by entering this command:
  config ipv6 neighbor-binding timers {**down-lifetime** | **reachable-lifetime** | **stale-lifetime**} {**enable** | **disable**}
- Configure the Unknown Address Multicast NS Forwarding by entering this command:
  config ipv6 ns-mcast-fwd {**enable** | **disable**}
- Configure NA Multicast Forwarding by entering this command:
  config ipv6 na-mcast-fwd {**enable** | **disable**}

  If you enable NA Multicast Forwarding, all unsolicited multicast NA from Wired/Wireless is not forwarded to Wireless.
- See the status of neighbor binding data that are configured on the controller by entering this command:
  show ipv6 neighbor-binding summary

802.3 Bridging

Information About Configuring 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.

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

Configuring 802.3 Bridging (GUI)

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)

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.

Fast SSID Change

Information About Configuring Fast SSID Changing

When fast SSID changing is enabled, the controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced.

When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID. When fast SSID is disabled and the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

Configuring Fast SSID Changing (GUI)

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

Step 2 From the Fast SSID Change drop-down list, choose **Enabled** to enable this feature or **Disabled** to disable it. The default value is disabled.

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

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

Configuring Fast SSID Changing (CLI)

Step 1 Enable or disable fast SSID changing by entering this command:
config network fast-ssid-change {**enable** | **disable**}

Step 2 Save your changes by entering this command:
save config

IP-MAC Address Binding

Information About Configuring IP-MAC Address Binding

The Cisco WLC 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. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.

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 WLC, 5508 WLC, 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 WLC, 5508 WLC, 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.

Configuring IP-MAC Address Binding (CLI)

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?>
```

AP TCP MSS Adjust

Information About Configuring the TCP 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 in controller software release 6.0 or later releases, 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.

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

Configuring TCP MSS (GUI)

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

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

Note The valid range are:

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

Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP .

Configuring TCP MSS (CLI)

Step 1 Enable or disable the TCP 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.

Note The valid ranges are:

- For IPv4 - Use a value between 536 and 1363 bytes.
- For IPv6 - Use a value between 1220 and 1331 bytes.

Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.

Step 2 Save your changes by entering this command:
save config

Step 3 See the current TCP 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   -
```