Advanced Wireless Tuning

Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

Note Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP does not respond with an association response bearing 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Note FlexConnect APs do support client load balancing.

Note For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the controller. A FlexConnect AP initially responds to the client before knowing the result of calculations at the controller. Load-balancing doesn't take effect when the FlexConnect AP is in standalone mode.

FlexConnect AP does not send (re)association response with status 17 for Load-Balancing as Local mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

This section contains the following subsections:

Configuring Aggressive Load Balancing (GUI)

Procedure

Step 1 Choose **Wireless** > **Advanced** > **Load Balancing** to open the Load Balancing page.

Step 2 In the Client Window Size text box, enter a value between 1 and 20.

The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 3 In the Maximum Denial Count text box, enter a value between 0 and 10.

The denial count sets the maximum number of association denials during load balancing.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 To enable or disable aggressive load balancing on specific WLANs, do the following:

a) Choose **WLANs** > **WLAN ID**. The WLANs > Edit page appears.
b) In the **Advanced** tab, select or unselect the **Client Load Balancing** check box.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring Aggressive Load Balancing (CLI)

Procedure

Step 1 Set the client window for aggressive load balancing by entering this command:

config load-balancing window *client_count*

You can enter a value between 0 and 20 for the *client_count* parameter.

Step 2 Set the denial count for load balancing by entering this command:

config load-balancing denial *denial_count*

You can enter a value between 1 and 10 for the *denial_count* parameter.

Step 3 Save your changes by entering this command:

save config

Step 4 Enable or disable aggressive load balancing on specific WLANs by entering this command:

config wlan load-balance allow {**enable** | **disable**} *wlan_ID*

You can enter a value between 1 and 512 for *wlan_ID* parameter.

Step 5 Verify your settings by entering this command:

show load-balancing

Step 6 Save your changes by entering this command:

save config

Step 7 Configure the load balance mode on a WLAN by entering this command:

config wlan load-balance mode {*client-count* | *uplink-usage*} *wlan-id*

This feature requires the AP to upload its uplink usage statistics to the controller periodically. Check these statistics by entering this command:

show ap stats system *cisco-AP*

Reanchoring of Roaming Voice Clients

You can allow voice clients to get anchored on the best suited and nearest available controller, which is useful when intercontroller roaming occurs. By using this feature, you can avoid the use of tunnels to carry traffic between the foreign controller and the anchor controller and remove unnecessary traffic from the network.

The ongoing call during roaming is not affected and can continue without any problem. The traffic passes through proper tunnels that are established between the foreign controller and the anchor controller. Disassociation occurs only after the call ends, and then the client then gets reassociated to a new controller.

Note You can reanchor roaming of voice clients for each WLAN.

This section contains the following subsections:

Restrictions for Configuring Reanchoring of Roaming Voice Clients

- The ongoing data session might be affected due to disassociation and then reassociation.
- This feature is supported for TSPEC-based calls and non-TSPEC SIP-based calls only when you enable the admission control.
- This feature is not recommended for use on Cisco 792x phones.

Configuring Reanchoring of Roaming Voice Clients (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure reanchoring of roaming voice clients.

Step 3 When the WLANs > Edit page appears, choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 In the Voice area select the **Re-anchor Roamed Clients** check box.

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

Step 6 Click **Save Configuration** to save your changes.

Configuring Reanchoring of Roaming Voice Clients (CLI)

Procedure

Step 1 Enable or disable reanchoring of roaming voice clients for a particular WLAN by entering this command:

config wlan roamed-voice-client re-anchor {enable | disable} *wlan id*

Step 2 Save your changes by entering this command:

save config

Step 3 See the status of reanchoring roaming voice client on a particular WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.............................. 1
Profile Name................................. wpa2-psk
Network Name (SSID).......................... wpa2-psk
Status....................................... Enabled
...
Call Snooping................................ Enabled
Roamed Call Re-Anchor Policy................. Enabled
Band Select.................................. Disabled
Load Balancing............................... Disabled
```

Step 4 Save your changes by entering this command:

save config

SpectraLink NetLink Telephones

For the best integration with the Cisco Wireless solution, SpectraLink NetLink Telephones require an extra operating system configuration step: **enable long preambles**.

The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

Enabling Long Preambles (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11b/g/n** > **Network** to open the 802.11b/g Global Parameters page.

Step 2 If the **Short Preamble** check box is selected, continue with this procedure. However, if the Short Preamble check box is unselected (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.

Step 3 Unselect the **Short Preamble** check box to enable long preambles.

Step 4 Click **Apply** to update the controller configuration.

Note If you do not already have an active CLI session to the controller, we recommend that you start a CLI session to reboot the controller and watch the reboot process. A CLI session is also useful because the GUI loses its connection when the controller reboots.

Step 5 Choose **Commands** > **Reboot** > **Reboot > Save and Reboot to reboot the controller**. Click OK in response to this prompt:

```
Configuration will be saved and the controller will be rebooted. Click ok to confirm.
```

The controller reboots.

Step 6 Log back onto the controller GUI to verify that the controller is properly configured.

Step 7 Choose **Wireless** > **802.11b/g/n** > **Network** to open the 802.11b/g Global Parameters page. If the **Short Preamble** check box is unselected, the controller is optimized for SpectraLink NetLink phones.

Enabling Long Preambles (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Enter the show 802.11b command and select the Short preamble mandatory parameter. If the parameter indicates that short preambles are enabled, continue with this procedure. This example shows that short preambles are enabled:

```
Short Preamble mandatory..................... Enabled
```

However, if the parameter shows that short preambles are disabled (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.

Step 3 Disable the 802.11b/g network by entering this command:

config 802.11b disable *network*

You cannot enable long preambles on the 802.11a network.

Step 4 Enable long preambles by entering this command:

config 802.11b preamble *long*

Step 5 Reenable the 802.11b/g network by entering this command:

config 802.11b *enable network*

Step 6 Enter the reset system command to reboot the controller. Enter y when the prompt to save the system changes is displayed. The controller reboots.

Step 7 Verify that the controller is properly configured by logging back into the CLI and entering the show 802.11b command to view these parameters:

```
802.11b Network.............................. Enabled
Short Preamble mandatory..................... Disabled
```

These parameters show that the 802.11b/g network is enabled and that short preambles are disabled.

Receiver Start of Packet Detection Threshold

Receiver Start of Packet Detection Threshold (Rx SOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity

decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network.

Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. Rx SOP helps to optimize the network performance at high-density deployments.

Note Rx SOP configuration is not applicable to 3rd radio module pluggable on 3600 AP.

Guidelines and Restrictions for RxSOP

- Configure this feature only if you have performed a complete site survey throughout your entire coverage area so that you know the RSSI at which all clients' signal levels are received at each AP.
- For information about support on various Wave 2 APs, see Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points.
- RxSOP configurations are supported only in Local, FlexConnect, Bridge, and Flex+Bridge modes.

  RxSOP configurations are not supported in the FlexConnect+PPPoE, FlexConnect+PPPoE-wIPS, and FlexConnect+OEAP submodes.

Configuring Rx SOP (GUI)

Procedure

Step 1 Choose **Wireless > Advanced > Rx SOP Threshold** to configure the high, medium, and low Rx SOP threshold values for each 802.11 band. The table below shows the Rx SOP threshold values for high, medium and low levels for each 802.11 band.

Table 1: Rx SOP Thresholds

802.11 Band	High Threshold	Medium Threshold	Low Threshold
5 GHz	-76 dBm	-78 dBm	-80 dBm
2.4 GHz	-79 dBm	-82 dBm	-85 dBm

Step 2 Choose **Wireless > RF Profiles** to configure the Rx SOP threshold value for an RF profile. The RF profiles page is displayed.

a) Click an RF profile to open the RF Profile > Edit page.
b) In the **High Density** tab, choose the Rx SOP threshold value from the **Rx SOP Threshold** drop-down list.

What to do next

Verify information about Rx SOP thresholds for an 802.11 band by using the**show** {**802.11a** | **802.11b**} **extended** command.

Configuring RxSOP (CLI)

Procedure

Step 1 Configure RxSOP threshold values for each 802.11 band by entering this command:

config {**802.11a | 802.11b** } **rx-sop threshhold** {**high | medium | low | default | custom**}

You can configure the RxSOP thresholds for an access point or on all access points in an 802.11 band.

Step 2 Configure RxSOP threshold values for an RF profile by entering this command:

config rf-profile rx-sop threshold {**high | medium | low | default | custom**} *profile_name*

Step 3 View information about RxSOP thresholds for an 802.11 band by entering this command:

show {**802.11a** | **802.11b**} **extended**

```
(Cisco Controller) > show 802.11a extended
Default 802.11a band Radio Extended Configurations:
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);

AP3600-XALE3  34:a8:4e:6a:7b:00
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);
AP54B4  3c:ce:73:6c:42:f0
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: -80;
```