Advanced Wireless Tuning

Band Selection

Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the controller.

Band selection works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In an access point, the band select table can be viewed by running the **show dot11 band-select** command. It can also be viewed by running the **show cont d0/d1 | begin Lru**command.

Note The WMM default configuration is not shown in the **show running-config** command output.

Band Selection Algorithm

The band selection algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to an access point, the corresponding client probe's Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- Scenario1: Client RSSI (as seen from the **show cont d0/d1** | **begin RSSI**command output) is greater than both Mid RSSI and Acceptable Client RSSI.
  - Dual-band clients: No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
  - Single-band (2.4-GHz) clients: 2.4-GHz probe responses are seen only after the probe suppression cycle.

- After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.

- Scenario2: Client RSSI (as seen from **show cont d0/d1** | **begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded to without any restrictions.
  - This scenario is similar to the band select disabled.

Note The client RSSI value (as seen in the **sh cont d0** | **begin RSSI** command output) is the average of the client packets received, and the Mid RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid RSSI value (7-dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

Restrictions for Band Selection

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1530, 1570,1700, 1800, 2700, 2800, 3700, 3800 Series APs.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Configuring Band Selection (GUI)

Procedure

Step 1 Choose **Wireless** > **Advanced** > **Band Select** to open the **Band Select** page.

Step 2 In the **Probe Cycle Count** text box, enter a value between 1 and 10. This cycle count sets the number of 2.4 GHz probe suppression cycles. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Scan Cycle Period Threshold (milliseconds)** text box, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle (i.e. only if the time difference between the successive probe requests is greater than this configured value, then the count value in the band select table increases). The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression (seconds)** text box, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 5 In the **Age Out Dual Band (seconds)** text box, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the **Acceptable Client RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 7 In the **Acceptable Client Mid RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the mid-RSSI, whose value can be used for toggling 2.4 GHz probe suppression based on the RSSI value. The default value is –60 dBm.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Step 10 To enable or disable band selection on specific WLANs, choose **WLANs** > **WLAN ID**. The **WLANs > Edit** page appears.

Step 11 Click the **Advanced** tab.

Step 12 In the **Load Balancing and Band Select** text area, if you want to enable band selection, select the **Client Band Select** check box. If you want to disable band selection, leave the check box unselected. The default value is disabled.

Step 13 Click **Save Configuration**.

Configuring Band Selection (CLI)

Procedure

Step 1 Set the probe cycle count for band select by entering this command:

config band-select cycle-count *cycle_count*

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

Step 2 Set the time threshold for a new scanning cycle period by entering this command:

config band-select cycle-threshold *milliseconds*

You can enter a value for threshold between 1 and 1000 for the *milliseconds* parameter.

Step 3 Set the suppression expire to the band select by entering this command:

config band-select expire suppression *seconds*

You can enter a value for suppression between 10 to 200 for the *seconds* parameter.

Step 4 Set the dual band expire by entering this command:

config band-select expire dual-band *seconds*

You can enter a value for dual band between 10 and 300 for the *seconds* parameter.

Step 5 Set the client RSSI threshold by entering this command:

config band-select client-rssi *client_rssi*

You can enter a value for minimum dBm of a client RSSI to respond to a probe between -20 and -90 for the *client_rssi* parameter.

Step 6 Set the client mid RSSI threshold by entering this command:

config band-select client-mid-rssi *client_mid_rssi*

You can enter a value for mid RSSI between -20 and -90 for the *client_mid_rssi* parameter.

Step 7 Enter the **save config** command to save your changes.

Step 8 Enable or disable band selection on specific WLANs by entering this command:

config wlan band-select allow {**enable** | **disable**} *wlan_ID*

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

Step 9 Verify your settings by entering this command:

show band-select

Information similar to the following appears:

```
Band Select Probe Response....................... Enabled
   Cycle Count................................... 3 cycles
   Cycle Threshold............................... 300 milliseconds
   Age Out Suppression........................... 20 seconds
   Age Out Dual Band............................. 20 seconds
   Client RSSI................................... -30 dBm
   Client Mid RSSI............................... -80 dBm
```

Step 10 Enter the **save config** command to save your changes.

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 Voice Client does not authenticate when delay is configured more than 300 ms. To avoid this configure a Central-Auth, Local Switching WLAN with CCKM, configure a Pagent Router between AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN and try associating the voice client

Passive scanning clients will be able to associate to an AP irrespective of whether load balancing is enabled or not.

Note With the 7.4 release, FlexConnect access points do support client load balancing.

You can configure the controller to analyze the WAN interface utilization of neighboring APs and then load balance the clients across the lightly loaded APs. You can configure this by defining a load balancing threshold. By defining the threshold, you can measure the WAN interface utilization percentage. For example, a threshold value of 50 triggers the load balancing upon detecting utilization of 50% or more on an AP-WAN interface.

Note For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the Cisco WLC. A FlexConnect AP initially responds to the client before knowing the result of calculations at the Cisco WLC. 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*

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.

Configuring Enhanced Distributed Channel Access (CLI)

To configure 802.11 enhanced distributed channel access (EDCA) parameters to support SpectraLink phones, use the following CLI commands:

config advanced edca-parameter {**custom-voice** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default**}

where

- **custom-voice** enables custom voice EDCA parameters
- **optimized-video-voice** enables combined video-voice-optimized parameters

- **optimized-voice** enables non-SpectraLink voice-optimized parameters
- **svp-voice** enables SpectraLink voice priority (SVP) parameters
- **wmm-default** enables wireless multimedia (WMM) default parameters

Note To propagate this command to all access points connected to the controller, make sure to disable and then reenable the 802.11b/g network after entering this command.

Information About 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 such as stadiums and auditoriums where access points need to optimize the nearest and strongest clients.

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

Restrictions for RxSOP

- RxSOP configurations are supported only on Cisco Aironet 2700, 2800, 3700, and 3800 series access points.
- The permitted range for the RxSOP threshold for the 5-GHz band is -76 dBm to -80 dBm and for the 2.4-GHz is -79 dBm to -85 dBm.

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

802.11 Band	High Threshold	Medium Threshold	Low Threshold
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;
```