Radio Resource Management

Information about Radio Resource Management

The Radio Resource Management (RRM) software embedded in the Cisco Wireless LAN Controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables Cisco WLCs to continually monitor their associated lightweight access points for the following information:

- Traffic load: The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference: The amount of traffic coming from other 802.11 sources.
- Noise: The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage: The received signal strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.

- Other: The number of nearby access points.

Using this information, RRM can periodically reconfigure the 802.11 RF network for best efficiency. To do this, RRM performs these functions:

- Radio resource monitoring
- Transmit power control
- Dynamic channel assignment
- Coverage hole detection and correction

Radio Resource Monitoring

RRM automatically detects and configures new Cisco WLCs and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can simultaneously scan all valid 5-GHz and 2.4-GHz channels for the country of operation as well as for channels available in other locations. The access points go "off-channel" for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

By default, each radio spends less than 2% of its time off channel.

Note Use off-channel scan deferral to prevent the AP from going off-channel when client traffic is active. For more information, see Off-Channel Scanning Deferral, on page 17.

Benefits of RRM

RRM produces a network with optimal capacity, performance, and reliability. It frees you from having to continually monitor the network for noise and interference problems, which can be transient and difficult to troubleshoot. RRM ensures that clients enjoy a seamless, trouble-free connection throughout the Cisco unified wireless network.

RRM uses separate monitoring and control for each deployed network: 5 GHz and 2.4 GHz. The RRM algorithms run separately for each radio type (5 GHz and 2.4 GHz). RRM uses both measurements and algorithms. RRM measurements can be adjusted using monitor intervals, but they cannot be disabled. RRM algorithms are enabled automatically but can be disabled by statically configuring channel and power assignment. The RRM algorithms run at a specified updated interval, which is 600 seconds by default.

Information About Configuring RRM

The controller's preconfigured RRM settings are optimized for most deployments. However, you can modify the controller's RRM configuration parameters at any time through either the GUI or the CLI.

You can configure these parameters on controllers that are part of an RF group or on controllers that are not part of an RF group.

The RRM parameters should be set to the same values on every controller in an RF group. The RF group leader can change as a result of controller reboots or depending on which radios hear each other. If the RRM parameters are not identical for all RF group members, varying results can occur when the group leader changes.

Using the controller GUI, you can configure the following RRM parameters: RF group mode, transmit power control, dynamic channel assignment, coverage hole detection, profile thresholds, monitoring channels, and monitor intervals.

Restrictions for Configuring RRM

- The Cisco 600 series OEAPs do not support RRM. The radios for the Cisco 600 series OEAPs are controlled through the local GUI of the Cisco 600 series OEAPs and not through the controller. Attempting to control the spectrum channel or power, or disabling the radios through the controller will fail to have any effect on the Cisco 600 series OEAPs.

Configuring RRM (CLI)

Procedure

Step 1 Disable the 802.11 network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 2 Choose the Transmit Power Control version by entering this command:

config advanced {**802.11a** | **802.11b**} **tpc-version** {**1** | **2**}

where:

- TPCv1: Coverage-optimal—(Default) Offers strong signal coverage and stability with negligible intercell interferences and sticky client syndrome.
- TPCv2: Interference-optimal—For scenarios where voice calls are extensively used. Tx power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there can be higher roaming delays and coverage hole incidents.

  Note TPCv2 is not supported.

Step 3 Perform one of the following to configure transmit power control:

- Have RRM automatically set the transmit power for all 802.11 radios at periodic intervals by entering this command:

  config {**802.11a** | **802.11b**} **txPower global auto**

- Have RRM automatically reset the transmit power for all 802.11a or 802.11b/g radios one time by entering this command:

  config {**802.11a** | **802.11b**} **txPower global once**

- Configure the transmit power range that overrides the Transmit Power Control algorithm, use this command to enter the maximum and minimum transmit power used by RRM:

  Note In Cisco WLC software release 7.6 or later releases, disabling the 802.11 network is not required for this command.

  config {**802.11a** | **802.11b**} **txPower global** {**max** | **min**} *txpower*

  where *txpower* is a value from –10 to 30 dBM. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

  If you configure a maximum transmit power, RRM does not allow any access point to exceed this transmit power (whether the maximum is set at RRM startup, or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually.

- Configure the Tx-Power Control to be aware of the channel by entering this command:

  config advanced {**802.11a** | **802.11b**} **tpcv1-chan-aware** {**enable** | **disable**}

  Note We recommend that you use this feature only on 802.11a (5-GHz) networks.

- Manually change the default transmit power setting by entering this command:

  config advanced {**802.11a** | **802.11b**} {**tpcv1-thresh** | **tpcv2-thresh**} *threshold*

  where *threshold* is a value from –80 to –50 dBm. Increasing this value causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect.

  In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients may have difficulty processing a large number of BSSIDs or a high beacon rate and may exhibit problematic behavior with the default threshold.

- Configure the Transmit Power Control Version 2 on a per-channel basis by entering this command:

  config advanced {**802.11a** | **802.11b**} **tpcv2-per-chan** {**enable** | **disable**}

Step 4 Perform one of the following to configure dynamic channel assignment (DCA):

- Have RRM automatically configure all 802.11 channels based on availability and interference by entering this command:

  config {**802.11a** | **802.11b**} **channel global auto**

- Have RRM automatically reconfigure all 802.11 channels one time based on availability and interference by entering this command:

  config {**802.11a** | **802.11b**} **channel global once**

- Disable RRM and set all channels to their default values by entering this command:

  config {**802.11a** | **802.11b**} **channel global off**

- Restart aggressive DCA cycle by entering this command:

config {**802.11a** | **802.11b**} **channel global restart**

- To specify the channel set used for DCA by entering this command:

  config advanced {**802.11a** | **802.11b**} **channel** {**add** | **delete**} *channel_number*

  You can enter only one channel number per command. This command is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Step 5 Configure additional DCA parameters by entering these commands:

- **config advanced** {**802.11a** | **802.11b**} **channel dca anchor-time** *value*—Specifies the time of day when the DCA algorithm is to start. value is a number between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.
- **config advanced** {**802.11a** | **802.11b**} **channel dca interval** *value*—Specifies how often the DCA algorithm is allowed to run. value is one of the following: 1, 2, 3, 4, 6, 8, 12, or 24 hours or 0, which is the default value of 10 minutes (or 600 seconds).

  Note If your Cisco WLC supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

- **config advanced** {**802.11a** | **802.11b**} **channel dca sensitivity** {**low** | **medium** | **high**}—Specifies how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channel.
  - **low** means that the DCA algorithm is not particularly sensitive to environmental changes.
  - **medium** means that the DCA algorithm is moderately sensitive to environmental changes.
  - **high** means that the DCA algorithm is highly sensitive to environmental changes.

The DCA sensitivity thresholds vary by radio band, as noted in following table.

Table 1: DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

- **config advanced 802.11a channel dca chan-width** {**20** | **40** | **80** | **80+80** }—Configures the DCA channel width for all 802.11n radios in the 5-GHz band.

  where

  - **20** sets the channel width for 802.11n radios to 20 MHz. This is the default value.
  - **40** sets the channel width for 802.11n radios to 40 MHz.

Note If you choose **40**, be sure to set at least two adjacent channels in the **config advanced 802.11a channel** {**add** | **delete**} *channel_number* command in *Step 4* (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for 40-MHz channel width.

Note If you choose 40, you can also configure the primary and extension channels used by individual access points.

Note To override the globally configured DCA channel width setting, you can configure an access point's radio mode using the **config 802.11a chan_width** *Cisco_AP* {**20** | **40** | **80**} command. If you change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

- **80** sets the channel width for the 802.11ac radios to 80 MHz.
- **80+80** sets the channel width for the 802.11 radio to 80+80 MHz.

- Configure slot-specific channel width by entering this command:

  config slot *slot-id* **chan_width***ap-name* {**20** | **40** | **80**}

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {***enable* **|** *disable***}**—Enables or disables to the Cisco WLC to avoid checks for non-DFS channels.

  Note This parameter is applicable only for deployments having outdoor access points such as 1522 and 1524.

- **config advanced** {**802.11a** | **802.11b**} **channel foreign** {**enable** | **disable**}—Enables or disables foreign access point interference avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel load** {**enable** | **disable**}—Enables or disables load avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel noise** {**enable** | **disable**}—Enables or disables noise avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel update**—Initiates an update of the channel selection for every Cisco access point.

Step 6 Configure coverage hole detection by entering these commands:

Note You can disable coverage hole detection on a per-WLAN basis.

- **config advanced** {**802.11a** | **802.11b**} **coverage** {**enable** | **disable**}—Enables or disables coverage hole detection. If you enable coverage hole detection, the Cisco WLC automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is enabled.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*—Specifies the minimum receive signal strength indication (RSSI) value for packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value below the value you

enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm for data packets and –75 dBm for voice packets. The access point takes RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

- **config advanced** {**802.11a** | **802.11b**} **coverage level global** *clients*—Specifies the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.
- **config advanced** {**802.11a** | **802.11b**} **coverage exception global** *percent*—Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **packet-count** *packets*—Specifies the minimum failure count threshold for uplink data or voice packets. The valid range is 1 to 255 packets, and the default value is 10 packets.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **fail-rate** *percent*—Specifies the failure rate threshold for uplink data or voice packets. The valid range is 1 to 100%, and the default value is 20%.

Note If both the number and percentage of failed packets exceed the values entered in the **packet-count** and **fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The Cisco WLC uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **coverage level global** and **coverage exception global** commands over a 90-second period. The Cisco WLC determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Step 7 Configure RRM NDP mode by entering this command:

config advanced 802.11{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**}

This command configures NDP mode. By default, the mode is set to “transparent”. The following options are available:

- Protected—Packets are encrypted.
- Transparent—Packets are sent as is.

Note See the discovery type by entering the **show advanced 802.11**{**a**|**b**} **monitor** command.

Step 8 Configure 802.11a or 802.11b/g network neighbor timeout-factor by entering this command:

config {**802.11a** | **802.11b**} **monitor timeout-factor** *factor-bw-5-to-60-minutes*

If you are using Release 8.1 or a later release, we recommend that you set the timeout factor to default 20. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes when the default NDP interval of 180s is in use, Cisco WLC deletes the neighbor from the neighbor list.

Note The Neighbor Timeout Factor was hardcoded to 60 minutes in Release 7.6, but was changed to 5 minutes in Release 8.0.100.0.

Step 9 Enable the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Note To enable the 802.11g network, enter **config 802.11b 11gSupport** *enable* after the **config 802.11b enable network** command.

Step 10 Save your settings by entering this command:

save config

Viewing RRM Settings (CLI)

Procedure

To see 802.11a and 802.11b/g RRM settings, use these commands:

show advanced {**802.11a** | **802.11b**} ?

where ? is one of the following:

- **ccx {***global* **|** *Cisco_AP***}**—Shows the CCX RRM configuration.
- **channel**—Shows the channel assignment configuration and statistics.
- **coverage**—Shows the coverage hole detection configuration and statistics.
- **logging**—Shows the RF event and performance logging.
- **monitor**—Shows the Cisco radio monitoring.
- **profile {***global* **|** *Cisco_AP***}**—Shows the access point performance profiles.
- **receiver**—Shows the 802.11a or 802.11b/g receiver configuration and statistics.
- **summary**—Shows the configuration and statistics of the 802.11a or 802.11b/g access points.
- **txpower**—Shows the transmit power assignment configuration and statistics.

RF Groups

Information About RF Groups

An RF group is a logical collection of controllers that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. Separate RF groups exist for 2.4-GHz and 5-GHz networks. Clustering WLCs into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single WLC .

An RF group is created based on the following parameters:

- User-configured RF network name.
- Neighbor discovery performed at the radio level.
- Country list configured on the controller.

RF grouping runs between MCs.

Lightweight access points periodically send out neighbor messages over the air. Access points using the same RF group name validate messages from each other.

When access points on different controllers hear validated neighbor messages at a signal strength of –80 dBm or stronger, the controllers dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group.

Note RF groups and mobility groups are similar, in that, they both define clusters of controllers , but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management, while a mobility group facilitates scalable, system-wide mobility and controller redundancy.

RF Group Leader

RF Group Leader can be configured in two ways as follows:

Note RF Group Leader is chosen on the basis of the controller with the greatest AP capacity (platform limit.) If multiple controllers have the same capacity, the leader is the one with the highest management IP address.

- Auto Mode: In this mode, the members of an RF group elect an RF group leader to maintain a *primary* power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or RF group members experience major changes).
- Static Mode: In this mode, a user selects a controller as an RF group leader manually. In this mode, the leader and the members are manually configured and fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the controllers in the RF group. The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

Note When a controller becomes both leader and member for a specific radio, you get to view the IPv4 and IPv6 address as part of the group leader.

When a Controller A becomes a member and Controller B becomes a leader, the Controller A displays either IPv4 or IPv6 address of Controller B using the address it is connected.

So, if both leader and member are not the same, you get to view only one IPv4 or IPv6 address as a group leader in the member.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

Note Several monitoring intervals are also available. See the Configuring RRM section for details.

RF Grouping Failure Reason Codes

RF Grouping failure reason codes and their explanations are listed below:

Table 2: RF Grouping Failure Reason Codes

Reason Code	Description
1	Maximum number (20) of controllers are already present in the group.
2	If the following conditions are met: • The request is from a similar powered controller and, • Controller is the leader for the other band, OR • Requestor group is larger.
3	Group ID do not match.
4	Request does not include source type.
5	Group spilt message to all member while group is being reformed.
6	Auto leader is joining a static leader, during the process deletes all the members.
9	Grouping mode is turned off.
11	Country code does not match.
12	Controller is up in hierarchy compared to sender of join command (static mode). Requestor is up in hierarchy (auto mode).

Reason Code	Description
13	Controller is configured as static leader and receives join request from another static leader.
14	Controller is already a member of static group and receives a join request from another static leader.
15	Controller is a static leader and receives join request from non-static member.
16	Join request is not intended to the controller. Controller name and IP do not match.
18	RF domain do not match.
19	Controller received a Hello packet at incorrect state.
20	Controller has already joined Auto leader, now gets a join request from static leader.
21	Group mode change. Domain name change from CLI. Static member is removed from CLI.
22	Max switch size (350) is reached

Additional Reference

Radio Resource Management White Paper: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_011.html

RF Group Name

A controller is configured in an RF group name, which is sent to all the access points joined to the controller and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the controllers to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a controller might hear RF transmissions from an access point on a different controller , you should configure the controller with the same RF group name. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

Controllers and APs in RF Groups

- Controller software supports up to 20 controllers and 6000 access points in an RF group.
- The RF group members are added based on the following criteria:

- Maximum number of APs Supported: The maximum limit for the number of access points in an RF group is 6000. The number of access points that are supported is determined by the number of APs licensed to operate on the controller.
- Twenty controllers: Only 20 controllers (including the leader) can be part of an RF group if the sum of the access points of all controllers combined is less than or equal to the upper access point limit.

Table 3: Controller Model Information

	8500	7500	5500	WiSM2
Maximum APs per RRM Group	6000	6000	1000	1000
Maximum AP Groups	6000	6000	500	500

Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

Note The RF group name is generally set at deployment time through the Startup Wizard. However, you can change it as necessary.

Note When the multiple-country feature is being used, all controllers intended to join the same RF group must be configured with the same set of countries, configured in the same order.

Note You can also configure RF groups using the Cisco Prime Infrastructure.

Configuring an RF Group Name (GUI)

Procedure

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

Step 2 Enter a name for the RF group in the RF-Network Name text box. The name can contain up to 19 ASCII characters.

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

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

Step 5 Repeat this procedure for each controller that you want to include in the RF group.

Configuring an RF Group Name (CLI)

Procedure

Step 1 Create an RF group by entering the **config network rf-network-name name** command:

Note For the group name, the limit is 19 ASCII characters.

Step 2 See the RF group by entering the **show network summary** command.

Step 3 Save your settings by entering the **save config** command.

Step 4 Repeat this procedure for each controller that you want to include in the RF group.

Configuring the RF Group Mode (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n> RRM > RF Grouping** to open the 802.11a (or 802.11b/g) RRM > RF Grouping page.

Step 2 From the **Group Mode** drop-down list, select the mode you want to configure for this controller.

You can configure RF grouping in the following modes:

- **auto**—Sets the RF group selection to automatic update mode.

  Note This mode does not support IPv6 based configuration.

- **leader**—Sets the RF group selection to static mode, and sets this controller as the group leader.

  Note Leader supports static IPv6 address.

  Note If a RF group member is configured using IPv4 address, then IPv4 address is used to communicate with the leader. The same is applicable for a RF group member configured using IPv6 too.

- **off**—Sets the RF group selection off. Every controller optimizes its own access point parameters.

  Note A configured static leader cannot become a member of another controller until its mode is set to **auto**.

Step 3 Click **Apply** to save the configuration and click **Restart** to restart RRM RF Grouping algorithm.

Step 4 If you configured RF Grouping mode for this controller as a static leader, you can add group members from the RF Group Members section as follows:

a. In the **Cisco WLC Name** field, enter the controller that you want to add as a member to this group.

b. In the **IP Address (IPv4/IPv6)** field, enter the IPv4/IPv6 address of the RF Group Member.

c. Click **Add Member** to add the member to this group.

Note If the member has not joined the static leader, the reason of the failure is shown in parentheses.

Step 5 Save the configuration.

Configuring the RF Group Mode (CLI)

Procedure

Step 1 Configure the RF Grouping mode by entering this command:

config advanced {**802.11a** | **802.11b**} **group-mode** {*auto* | *leader* | *off* | *restart*}

- *auto*—Sets the RF group selection to automatic update mode.
- *leader*—Sets the RF group selection to static mode, and sets this controller as the group leader.

  Note If a group member is configured with IPv4 address, then IPv4 address is used to communicate with a leader and vice versa with IPv6 also.

- *off*—Sets the RF group selection off. Every controller optimizes its own access point parameters.
- *restart*—Restarts the RF group selection.

  Note A configured static leader cannot become a member of another controller until its mode is set to *auto*.

Step 2 Add or remove a controller as a static member of the RF group (if the mode is set to *leader*) by entering these commands:

- **config advanced** {**802.11a** | **802.11b**} **group-member add** *controller-name ipv4-or-ipv6-address*
- **config advanced** {**802.11a** | **802.11b**} *group-member* **remove** *controller-name ipv4-or-ipv6-address*

Note You can add RF Group Members using either IPv4 or IPv6 address.

Step 3 See RF grouping status by entering this command:

show advanced {**802.11a** | **802.11b**} *group*

Viewing RF Group Status

Viewing the RF Group Status (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** > **or 802.11b/g/n > RRM** > **RF Grouping** to open the 802.11a/n/ac (or 802.11b/g/n) RRM > RF Grouping page.

This page shows the details of the RF group, displaying the configurable parameter **RF Group mode**, the **RF Group role** of this Cisco WLC, the **Update Interval** and the Cisco WLC name and IP address of the **Group Leader** to this Cisco WLC.

Note RF grouping mode can be set using the **Group Mode** drop-down list.

Tip Once a Cisco WLC has joined as a static member and you want to change the grouping mode, we recommend that you remove the member from the configured static-leader and also make sure that a member Cisco WLC has not been configured to be a member on multiple static leaders. This is to avoid repeated join attempts from one or more RF static leaders.

Step 2 (Optional) Repeat this procedure for the network type that you did not select (802.11a/n/ac or 802.11b/g/n).

Viewing the RF Group Status (CLI)

Procedure

Step 1 See which controller is the RF group leader for the 802.11a RF network by entering this command:

show advanced 802.11a group

Information similar to the following appears:

```
Radio RF Grouping
  802.11a Group Mode..................... STATIC
  802.11a Group Update Interval.......... 600 seconds
  802.11a Group Leader................... test (209.165.200.225)
    802.11a Group Member................... test (209.165.200.225)
  802.11a Last Run....................... 397 seconds ago
```

This output shows the details of the RF group, specifically the grouping mode for the controller, how often the group information is updated (600 seconds by default), the IP address of the RF group leader, the IP address of this controller, and the last time the group information was updated.

Note If the IP addresses of the group leader and the group member are identical, this controller is currently the group leader.

Note A * indicates that the controller has not joined as a static member.

Step 2 See which controller is the RF group leader for the 802.11b/g RF network by entering this command:

show advanced 802.11b group

Rogue Access Point Detection in RF Groups

After you have created an RF group of controller , you need to configure the access points connected to the controller to detect rogue access points. The access points will then select the beacon or probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the selection is successful, the frames are authenticated. Otherwise, the

authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the controller .

Enabling Rogue Access Point Detection in RF Groups (GUI)

Procedure

Step 1 Make sure that each controller in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the controllers have different names, false alarms will occur.

Step 2 Choose **Wireless** to open the All APs page.

Step 3 Click the name of an access point to open the All APs > Details page.

Step 4 Choose either **local** or **monitor** from the AP Mode drop-down list and click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Step 6 Repeat Step 2 through Step 5 for every access point connected to the controller.

Step 7 Choose **Security** > **Wireless Protection Policies** > **AP Authentication/MFP** to open the AP Authentication Policy page.

The name of the RF group to which this controller belongs appears at the top of the page.

Step 8 Choose **AP Authentication** from the Protection Type drop-down list to enable rogue access point detection.

Step 9 Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

Note The valid threshold range is from1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Step 12 Repeat this procedure on every controller in the RF group.

Note If rogue access point detection is not enabled on every controller in the RF group, the access points on the controllers with this feature disabled are reported as rogues.

Configuring Rogue Access Point Detection in RF Groups (CLI)

Procedure

Step 1 Make sure that each controller in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the controllers have different names, false alarms will occur.

Step 2 Configure a particular access point for local (normal) mode or monitor (listen-only) mode by entering this command:

config ap mode local *Cisco_AP* or **config ap mode monitor** *Cisco_AP*

Step 3 Save your changes by entering this command:

save config

Step 4 Repeat *Step 2* and *Step 3* for every access point connected to the controller.

Step 5 Enable rogue access point detection by entering this command:

config wps ap-authentication

Step 6 Specify when a rogue access point alarm is generated by entering this command. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

config wps ap-authentication *threshold*

Note The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 7 Save your changes by entering this command:

save config

Step 8 Repeat *Step 5* through *Step 7* on every controller in the RF group.

Note If rogue access point detection is not enabled on every controller in the RF group, the access points on the controllers with this feature disabled are reported as rogues.

Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 milliseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is

received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples are marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

Configuring Off-Channel Scanning Deferral for WLANs

Configuring Off-Channel Scanning Deferral for a WLAN (GUI)

Procedure

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

Step 2 Click the WLAN ID.

Step 3 Choose the **Advanced** tab from the **WLANs > Edit** page.

Step 4 In the **Off Channel Scanning Defer** section, set the **Scan Defer Priority** by clicking on the priority argument.

Step 5 Set the time in milliseconds in the **Scan Defer Time** field.

Valid values are between 0 and 60000 milliseconds; the default value is 100 milliseconds. If you sent the time to 0, the scan deferral does not happen.

The scan defer time is common for all priorities on the same WLAN and the scan is deferred if a packet is transmitted or received in any one of the defer priorities.

Step 6 Save the configuration.

Configuring Off Channel Scanning Deferral for a WLAN (CLI)

Procedure

Step 1 Assign a defer-priority for the channel scan by entering this command:

config wlan channel-scan defer-priority *priority-value* {**enable** | **disable**} *wlan-id*

Valid priority value is between 0 and 7 (this value should be set to 6 on the client and on the WLAN).

Use this command to configure the amount of time that scanning will be deferred following an UP packet in the queue.

Step 2 Assign the channel scan defer time (in milliseconds) by entering this command:

config wlan channel-scan defer-time *time-in-msecswlan-id*

The time value is in milliseconds (ms) and the valid range is between 0 and 60000 ms (60 seconds); the default value is 100 ms. This setting should match the requirements of the equipment on your WLAN. If you sent the time to 0, the scan deferral does not happen.

The scan defer time is common for all priorities on the same WLAN and the scan is deferred if a packet is transmitted or received in any one of the defer priorities.

RRM NDP and RF Grouping

The Cisco Neighbor Discovery Packet (NDP) is the fundamental tool for RRM and other wireless applications that provides information about the neighbor radio information. You can configure the controller to encrypt neighbor discovery packets.

An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.

Guidelines

- This feature enables you to be compliant with the PCI specifications.
- An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.
- Ensure that the Cisco Wave 2 APs have an SSID enabled for the APs to send NDP packets. If only the AP radios are enabled but not SSID, then the APs cannot send NDP packets and thus RRM does not work as expected.

Configuring RRM NDP (CLI)

Procedure

Step 1 To configure RRM NDP using the controller CLI, enter this command:

config advanced 802.11{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**}

This command configures NDP mode. By default, the mode is set to *transparent*. The following options are available:

- Protected: Packets are encrypted.
- Transparent: Packets are sent as is.

Step 2 To configure RRM NDP using the controller CLI, enter this command:

show advanced 802.11{a|b} monitor

Channels

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Controllers can dynamically allocate access point channel assignments to avoid conflict and increase capacity and performance. Channels are *reused* to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The controller's Dynamic Channel Assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot simultaneously use 11 or 54 Mbps. By effectively reassigning channels, the controller keeps adjacent channels that are separated.

Note We recommend that you use only nonoverlapping channels (1, 6, 11, and so on).

Note Channel change does not require you to shut down the radio.

The controller examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- Access point received energy: The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.
- Noise: Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the controller can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.
- 802.11 interference: Interference is any 802.11 traffic that is not a part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all the channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the controller. Using

the RRM algorithms, the controller may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

In addition, if other wireless networks are present, the controller shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the controller may choose to avoid this channel. In huge deployments in which all nonoverlapping channels are occupied, the controller does its best, but you must consider RF density when setting expectations.

- Load and utilization: When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points, for example, a lobby versus an engineering area. The controller can then assign channels to improve the access point that has performed the worst. The load is taken into account when changing the channel structure to minimize the impact on the clients that are currently in the wireless LAN. This metric keeps track of every access point's transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This *Load and utilization* parameter is disabled by default.

The controller combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

Note Radios using 40-MHz channels in the 2.4-GHz band or 80MHz channels are not supported by DCA.

Note In a Dynamic Frequency Selection (DFS) enabled AP environment, ensure that you enable the UNII2 channels option under the DCA channel to allow 100-MHz separation for the dual 5-GHz radios.

The RRM startup mode is invoked in the following conditions:

- In a single-controller environment, the RRM startup mode is invoked after the controller is upgraded and rebooted.
- In a multiple-controller environment, the RRM startup mode is invoked after an RF Group leader is elected.
- You can trigger the RRM startup mode from the CLI.

The RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady-state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Note DCA algorithm interval is set to 1 hour, but DCA algorithm always runs in default interval of 10 min, channel allocation occurs at 10-min intervals for the first 10 cycles, and channel changes occur as per the DCA algorithm every 10 min. After that the DCA algorithm goes back to the configured time interval. This is common for both DCA interval and anchor time because it follows the steady state.

Note If Dynamic Channel Assignment (DCA)/Transmit Power Control (TPC) is turned off on the RF group member, and auto is set on RF group leader, the channel or TX power on a member gets changed as per the algorithm that is run on the RF group leader.

Configuring Dynamic Channel Assignment (GUI)

You can specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning by using the controller GUI.

Note This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Procedure

Step 1 Disable the 802.11a/n/ac or 802.11b/g/n network as follows:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the **Global Parameters** page.
b) Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.
c) Click **Apply**.

Step 2 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **DCA** to open the **Dynamic Channel Assignment (DCA)** page.

Step 3 Choose one of the following options from the **Channel Assignment Method** drop-down list to specify the controller's DCA mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.
- **Freeze**—Causes the controller to evaluate and update the channel assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**.

  Note The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.

  Note For optimal performance, we recommend that you use the Automatic setting.

Step 4 From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: **10 minutes**, **1 hour**, **2 hours**, **3 hours**, **4 hours**, **6 hours**, **8 hours**, **12 hours**, or **24 hours**. The default value is 10 minutes.

Note If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

Step 5 From the AnchorTime drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 6 Check the **Avoid Foreign AP Interference** check box to cause the controller's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is selected.

Step 7 Check the **Avoid Cisco AP Load** check box to cause the controller's RRM algorithms to consider 802.11 traffic from APs in your wireless network when assigning channels, or uncheck it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is unselected.

Step 8 Check the **Avoid Non-802.11a (802.11b) Noise** check box to cause the controller's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is selected.

Step 9 Check the **Avoid Persistent Non-WiFi Interference** check box to configure the controller to stop ignoring persistent non-Wi-Fi interference in new channel calculation. The persistent non-Wi-Fi interference is considered during the metric calculation for channels.

Step 10 From the **DCA Channel Sensitivity** drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low**—The DCA algorithm is not particularly sensitive to environmental changes.
- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.
- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is Medium. The DCA sensitivity thresholds vary by radio band, as noted in the table below.

Table 4: DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

Step 11 For 802.11a/n/ac networks only, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth.

- **40 MHz**—The 40-MHz channel bandwidth

Note If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List in *Step 13* (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

Note If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points.

Note To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode on the 802.11a/n Cisco APs > Configure page. if you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

Note The FlexDFS functionality in this context is as follows:

Suppose RADAR is detected on an AP channel and the AP channel width is set to 40 MHz and global width is set to 80 MHz. One of the following scenarios occurs:

- If the RADAR is detected on the primary channel, the channel width changes to the globally configured value, that is 80 MHz, and a new channel is assigned.
- If the RADAR is detected on the secondary channel, the channel width changes to half of the existing width, that is 20 MHz.
- If the RADAR is detected on both the primary and secondary channels, the channel width changes to the globally configured value, that is 80 MHz, and a new channel is assigned.

Note If you choose 40 MHz on the 802.11a radio, you cannot pair channels 116, 140, and 165 with any other channels.

- **80 MHz**—The 80-MHz bandwidth for the 802.11ac radios.
- **160 MHz**—The 160-MHz bandwidth for 802.11ac radios.
- **best**—It selects the best bandwidth suitable. This option is enabled for the 5-GHz radios only.

This page also shows the following nonconfigurable channel parameter settings:

- Channel Assignment Leader—The MAC address of the RF group leader, which is responsible for channel assignment.
- Last Auto Channel Assignment—The last time RRM evaluated the current channel assignments.

Step 12 Select the **Avoid check for non-DFS** channel to enable the controller to avoid checks for non-DFS channels. DCA configuration requires at least one non-DFS channel in the list. In the EU countries, outdoor deployments do not support non-DFS channels. Customers based in EU or regions with similar regulations must enable this option or at least have one non-DFS channel in the DCA list even if the channel is not supported by the APs.

Note This parameter is applicable only for deployments having outdoor access points such as 1522 and 1524.

Step 13 In the **DCA Channel List** area, the **DCA Channels** field shows the channels that are currently selected. To choose a channel, check its check box in the **Select** column. To exclude a channel, uncheck its check box.

The ranges are as follows: 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165, 190, 196 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

The defaults are as follows: 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161 802.11b/g—1, 6, 11

Note Depending on the countries configured on the controller, only a subset of the channels are available.

Step 14 If you are using Cisco Aironet 1520 series mesh access points in your network, you need to set the 4.9-GHz channels in the 802.11a band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, check its check box in the **Select** column. To exclude a channel, uncheck its check box.

The ranges are as follows: 802.11a—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26

Step 15 Click **Apply**.

Step 16 Reenable the 802.11 networks as follows:

a. Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the Global Parameters page.

b. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply**.

Step 17 If you have implemented major changes to your wireless network, such as installing new APs or changing your channel plan, you must now run the startup mode. You can do this in the CLI by entering this command:

config {**802.11a** | **802.11b**} **channel global restart**

Step 18 Click **Save Configuration**.

Note To see why the DCA algorithm changed channels, choose **Monitor** and then choose **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Configuring RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **General** to open the 802.11a/n/ac (or 802.11b/g/n) > RRM > General page.

Step 2 Configure profile thresholds used for alarming as follows:

Note The profile thresholds have no bearing on the functionality of the RRM algorithms. Lightweight access points send an SNMP trap (or an alert) to the Cisco WLC when the values set for these threshold parameters are exceeded.

a) In the **Interference** text box, enter the percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. The valid range is 0 to 100%, and the default value is 10%.
b) In the **Clients** text box, enter the number of clients on a single access point. The valid range is 1 to 200, and the default value is 12.
c) In the **Noise** text box, enter the level of noise (non-802.11 traffic) on a single access point. The valid range is –127 to 0 dBm, and the default value is –70 dBm.
d) In the **Utilization** text box, enter the percentage of RF bandwidth being used by a single access point. The valid range is 0 to 100%, and the default value is 80%.

Step 3 From the **Channel List** drop-down list, choose one of the following options to specify the set of channels that the access point uses for RRM scanning:

- **All Channels**—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
- **Country Channels**—RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
- **DCA Channels**—RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired. To do so, follow instructions in the Dynamic Channel Assignment.

Note Neighbor Discovery Protocol (NDP) request is sent only on Dynamic Channel Assignment (DCA) channels.

Step 4 Configure monitor intervals as follows:

a. In the **Channel Scan Interval** box, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at the interval configured here. The time spent listening on each channel is determined by the non-configurable 50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms is spent listening on each scanned channel (180/11 = ~16 seconds). The Channel Scan Interval parameter determines the interval at which the scanning occurs.The valid range is 60 to 3600 seconds, and the default value is 60 seconds for 802.11a radios and 180 seconds for the 802.11b/g radios.

Note If your Cisco WLC supports only OfficeExtend access points, we recommend that you set the channel scan interval to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

b. In the **Neighbor Packet Frequency** box, enter (in seconds) how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default value is 60 seconds.

Note If your Cisco WLC supports only OfficeExtend access points, we recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

c. In the **Neighbor Timeout Factor** box, enter the NDP timeout factor value in minutes. The valid range is 5 minutes to 60 minutes with the default value being 5 minutes.

If you are using Release 8.1 or a later release, we recommend that you set the timeout factor to default 20. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes when the default NDP interval of 180s is in use, Cisco WLC deletes the neighbor from the neighbor list.

Note The Neighbor Timeout Factor was hardcoded to 60 minutes in Release 7.6, but was changed to 5 minutes in Release 8.0.100.0.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Note Click **Set to Factory Default** if you want to return all of the Cisco WLC's RRM parameters to their factory-default values.

Overriding RRM

In some deployments, it is desirable to statically assign channel and transmit power settings to the access points instead of relying on the RRM algorithms provided by Cisco. Typically, this is true in challenging RF environments and non standard deployments but not the more typical carpeted offices.

Note If you choose to statically assign channels and power levels to your access points and/or to disable dynamic channel and power assignment, you should still use automatic RF grouping to avoid spurious rogue device events.

You can disable dynamic channel and power assignment globally for a Cisco WLC, or you can leave dynamic channel and power assignment enabled and statically configure specific access point radios with a channel and power setting. While you can specify a global default transmit power parameter for each network type that applies to all the access point radios on a Cisco WLC, you must set the channel for each access point radio when you disable dynamic channel assignment. You may also want to set the transmit power for each access point instead of leaving the global transmit power in effect.

This section contains the following subsections:

Statically Assigning Channel and Transmit Power Settings (GUI)

Procedure

Step 1 Choose **Wireless > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

This page shows all the 802.11a/n/ac or 802.11b/g/n access point radios that are joined to the Cisco WLC and their current settings. The Channel text box shows both the primary and extension channels and uses an asterisk to indicate if they are globally assigned.

Step 2 Hover your cursor over the blue drop-down arrow for the access point for which you want to modify the radio configuration and choose **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page appears.

Step 3 Specify the RF Channel Assignment from the following options:

- **Global**—Choose this to specify a global value.
- **Custom**—Choose this and then select a value from the adjacent drop-down list to specify a custom value.

Step 4 Configure the antenna parameters for this radio as follows:

a. From the Antenna Type drop-down list, choose **Internal** or **External** to specify the type of antennas used with the access point radio.

b. Select and unselect the check boxes in the Antenna text box to enable and disable the use of specific antennas for this access point, where A, B, and C are specific antenna ports. The D antenna appears for the Cisco 3600 Series Access Points. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from antenna ports A and B and receptions from antenna port C, you would select the following check boxes: Tx: A and B and Rx: C. In 3600 APs, the valid combinations are A, A+B, A+B+C or A+B+C+D. When you select a dual mode antenna, you can only apply single spatial 802.11n stream rates: MCS 0 to 7 data rates. When you select two dual mode antennae, you can apply only the two spatial 802.11n stream rates: MCS 0 to 15 data rates.

c. In the Antenna Gain text box, enter a number to specify an external antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (see *Cisco Aironet Antenna Reference Guide* for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The Cisco WLC reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations.

d. Choose one of the following options from the Diversity drop-down list:

Enabled—Enables the antenna connectors on both sides of the access point. This is the default value.

Side A or Right—Enables the antenna connector on the right side of the access point.

Side B or Left—Enables the antenna connector on the left side of the access point.

Step 5 In the RF Channel Assignment area, choose **Custom** for the Assignment Method under RF Channel Assignment and choose a channel from the drop-down list to assign an RF channel to the access point radio.

Step 6 In the Tx Power Level Assignment area, choose the **Custom** assignment method and choose a transmit power level from the drop-down list to assign a transmit power level to the access point radio.

The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

Note See the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, see the data sheet for your access point for the number of power levels supported.

Note If the access point is not operating at full power, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section.

Step 7 Choose **Enable** from the Admin Status drop-down list to enable this configuration for the access point.

Step 8 Click **Apply**.

Step 9 Have the Cisco WLC send the access point radio admin state immediately to Cisco Prime Infrastructure as follows:

a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Select the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply**.

Step 10 Click **Save Configuration**.

Step 11 Repeat this procedure for each access point radio for which you want to assign a static channel and power level.

Statically Assigning Channel and Transmit Power Settings (CLI)

Procedure

Step 1 Disable the radio of a particular access point on the 802.11a/n/ac or 802.11b/g/n network by entering this command:

config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

Step 2 Configure the channel width for a particular access point by entering this command:

config {**802.11a** | **802.11b**} **chan_width** *Cisco_AP* {**20** | **40** | **80**}

where

- **20** allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.

- **40** allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the Cisco WLC would use channel 48 as the extension channel. If you choose a primary channel of 48, the Cisco WLC would use channel 44 as the extension channel.

  Note This parameter can be configured only if the primary channel is statically assigned.

  Note Statically configuring an AP's radio for one of the available modes overrides the globally configured DCA channel width setting (configured using the **config advanced 802.11a channel dca chan-width-11n** {**20** | **40** | **80**} command). If you ever change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

- **80** sets the channel width for the 802.11ac radios to 80 MHz.

Note Channels 116, 120, 124, and 128 are not available in the U.S. and Canada for 40-MHz channel bonding.

Note You should disable the operational and admin status of the slot 1 and slot 2 on the Cisco Aironet 3600 Series APs with 802.11 ac module before changing the channel width using the **config 802.11 {a | b} chan_width ap** *ap-name channel* command. We recommend that you use the **config 802.11 {a | b} disable ap** command to disable the operational and admin status.

Step 3 Enable or disable the use of specific antennas for a particular access point by entering this command:

config {**802.11a** | **802.11b**} **11nsupport antenna** {**tx** | **rx**} *Cisco_AP* {**A** | **B** | **C**} {**enable** | **disable**}

where A, B, and C are antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from the antenna in access point AP1's antenna port C on the 802.11a network, you would enter this command:

config 802.11a 11nsupport antenna tx AP1 C enable

Note You cannot enable or disable individual antennas for 802.11ac because the 802.11ac module antennas are internal.

Step 4 Specify the external antenna gain, which is a measure of an external antenna's ability to direct or focus radio energy over a region of space entering this command:

config {**802.11a** | **802.11b**} **antenna extAntGain** *antenna_gain Cisco_AP*

High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (see *Cisco Aironet Antenna Reference Guide* for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The Cisco WLC reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations.

Step 5 Configure beamforming for the 5-GHz radios for all APs or a specific by entering this command:

config 802.11a {**global** | **ap** *ap-name*} {**enable** | **disable**}

Step 6 Specify the channel that a particular access point is to use by entering this command:

config {**802.11a** | **802.11b**} **channel ap** *Cisco_AP channe*l

For example, to configure 802.11a channel 36 as the default channel on AP1, enter the **config 802.11a channel ap AP1 36** command.

The channel you choose is the primary channel (for example, channel 36), which is used for communication by legacy 802.11a radios and 802.11n 20-MHz radios. 802.11n 40-MHz radios use this channel as the primary channel but also use an additional bonded extension channel for faster throughput, if you chose 40 for the channel width.

Note Changing the operating channel causes the access point radio to reset.

Step 7 Specify the transmit power level that a particular access point is to use by entering this command:

config {**802.11a** | **802.11b**} **txPower ap** *Cisco_AP power_level*

For example, to set the transmit power for 802.11a AP1 to power level 2, enter the **config 802.11a txPower ap AP1 2** command.

The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

In certain cases, Cisco access points support only 7 power levels for certain channels, so that the Cisco Wireless Controller considers the 7th and 8th power levels as the same. If the 8th power level is configured on those channels, the configuration would fail since the controller considers the 7th power level as the lowest acceptable valid power level. These power values are derived based on the regulatory compliance limits and minimum hardware limitation which varies across different Cisco access points. For example, Cisco 3500, 1140, and 1250 series access points allow the configuration of last power levels because those access points report the "per path power" to the controller, whereas all next generation acess points such as Cisco 3700, 3600, 2600, and 1600 series access points report "total power value" to the controller, thereby decreasing the allowed power levels for newer generation products. For example, if the last power level in the 3600E access point has a power value of 4dbm (total power), then it actually means the power value is -2dbm (per path).

Note See the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, see data sheet for your access point for the number of power levels supported.

Step 8 Save your settings by entering this command:

save config

Step 9 Repeat *Step 2* through *Step 7* for each access point radio for which you want to assign a static channel and power level.

Step 10 Reenable the access point radio by entering this command:

config {**802.11a** | **802.11b**} **enable** *Cisco_AP*

Step 11 Have the Cisco WLC send the access point radio admin state immediately to WCS by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Step 12 Save your changes by entering this command:

save config

Step 13 See the configuration of a particular access point by entering this command:

show ap config {**802.11a** | **802.11b**} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 7
Cisco AP Name.................................... AP1
...
Tx Power
Num Of Supported Power Levels ............. 8
      Tx Power Level 1 ........................... 20 dBm
      Tx Power Level 2 ........................... 17 dBm
      Tx Power Level 3 ........................... 14 dBm
      Tx Power Level 4 ........................... 11 dBm
      Tx Power Level 5 ........................... 8 dBm
      Tx Power Level 6 ........................... 5 dBm
      Tx Power Level 7 ........................... 2 dBm
      Tx Power Level 8 ........................... -1 dBm
      Tx Power Configuration ..................... CUSTOMIZED
      Current Tx Power Level ..................... 1

Phy OFDM parameters
      Configuration .............................. CUSTOMIZED
      Current Channel ............................ 36
      Extension Channel .......................... 40
      Channel Width.............................. 40 Mhz
      Allowed Channel List....................... 36,44,52,60,100,108,116,132,
        ......................................... 149,157
      TI Threshold ............................... -50
      Antenna Type............................... EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBi units).... 7
      Diversity.................................. DIVERSITY_ENABLED

802.11n Antennas
        Tx
         A..................................... ENABLED
         B..................................... ENABLED
        Rx
         A..................................... DISABLED
         B..................................... DISABLED
         C..................................... ENABLED
```

Disabling Dynamic Channel and Power Assignment (CLI)

Procedure

Step 1 Disable the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 2 Disable RRM for all 802.11a or 802.11b/g radios and set all channels to the default value by entering this command:

config {**802.11a** | **802.11b**} **channel global off**

Step 3 Enable the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Note To enable the 802.11g network, enter the **config 802.11b 11gSupport enable** command after the **config 802.11b enable network** command.

Step 4 Save your changes by entering this command:

save config

802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

Configuring the 802.11h Parameters (GUI)

Procedure

Step 1 Disable the 802.11 band as follows:

a) Choose **Wireless > 802.11a/n/ac > Network** to open the **802.11a Global Parameters** page.
b) Unselect the **802.11a Network Status** check box.
c) Click **Apply**.

Step 2 Choose **Wireless > 802.11a/n/ac > DFS (802.11h)** to open the **802.11h Global Parameters** page.

Step 3 In the Power Constraint area, enter the local power constraint. The valid range is between 0 dBm and 30 dBm.

Step 4 In the Channel Switch Announcement area, select the **Channel Announcement** check box if you want the access point to announce when it is switching to a new channel and the new channel number, or unselect this check box to disable the channel announcement. The default value is disabled.

Step 5 If you enabled the channel announcement, the **Channel Quiet Mode** check box appears. Select this check box if you want the access point to stop transmitting on the current channel, or unselect this check box to disable quiet mode. The default value is disabled.

Step 6 Click **Apply**.

Step 7 Reenable the 802.11a band as follows:

a) Choose **Wireless > 802.11a/n/ac > Network** to open the **802.11a Global Parameters** page.
b) Select the **802.11a Network Status** check box.
c) Click **Apply**.

Step 8 Click **Save Configuration**.

Configuring the 802.11h Parameters (CLI)

Procedure

Step 1 Disable the 802.11a network by entering this command:

config 802.11a disable network

Step 2 Enable or disable an access point to announce when it is switching to a new channel, and the new channel number by entering this command:

config 802.11h channelswitch {**enable** {**loud** | **quiet**} | **disable**}

Enter either **quiet** or **loud** for the **enable** parameter. When the quiet mode is enabled, all the clients who can enable 802.11h channel switch announcements should stop transmitting packets immediately because the AP detects that the radar and client devices should also quit transmitting to reduce interference. By default, the Channel Switch feature is in disabled state.

Step 3 Configure a new channel using the 802.11h channel announcement by entering this command:

config 802.11h setchannel channel *channel*

Step 4 Configure the 802.11h power constraint value by entering this command:

config 802.11h powerconstraint *value*

Use increments of 3 dB for the value so that the AP goes down one power level at a time.

Step 5 Reenable the 802.11a network by entering this command:

config 802.11a enable network

Step 6 View the status of the 802.11h parameters by entering this command:

show 802.11h

Information similar to the following appears:

```
Power Constraint................................ 0
Channel Switch.................................. Disabled
Channel Switch Mode............................. 0
```

Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions.

The Transmit Power Control (TPC) algorithm increases and decreases an access point’s power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage, for example, if an access point fails or becomes disabled, TPC can also increase power on the surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve the required coverage levels while avoiding channel interference between access points. We recommend

that you select TPCv1; TPCv2 option is deprecated. With TPCv1, you can select the channel aware mode; we recommend that you select this option for 5 GHz, and leave it unchecked for 2.4 GHz.

These documents provide more information on Transmit Power Control values for the following access points:

Cisco Aironet 3500 Series http://www.cisco.com/c/en/us/support/wireless/aironet-3500-series/products-installation-guides-list.html

Cisco Aironet 3700 Series http://www.cisco.com/c/en/us/support/wireless/aironet-3700-series/products-installation-guides-list.html

Cisco Aironet 700 Series http://www.cisco.com/c/en/us/support/wireless/aironet-700-series/products-installation-guides-list.html

Cisco Aironet 1530 Series http://www.cisco.com/c/en/us/support/wireless/aironet-1530-series/products-installation-guides-list.html

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions, for example, when all the access points must be mounted in a central hallway, placing the access points close together, but requiring coverage to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all the access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment, enter the maximum and minimum transmit power used by RRM in the fields in the **Tx Power Control** window. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the controller, to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, no access point will transmit above 11 dBm, unless the access point is configured manually.

Configuring Transmit Power Control (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **TPC** to open the 802.11a/n/ac (or 802.11b/g/n) > RRM > Tx Power Control (TPC) page.

Step 2 Choose the Transmit Power Control version from the following options:

- Interference Optimal Mode (TPCv2)—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

Note We recommend that you use TCPv2 only in cases where RF issues cannot be resolved by using TCPv1. Please evaluate and test the use of TPCv2 with the assistance of Cisco Services.

- Coverage Optimal Mode (TPCv1)—(Default) Offers strong signal coverage and stability. In this mode, power can be kept low to gain extra capacity and reduce interference.

Step 3 Choose one of the following options from the Power Level Assignment Method drop-down list to specify the Cisco WLC's dynamic power assignment mode:

- **Automatic**—Causes the Cisco WLC to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
- **On Demand**—Causes the Cisco WLC to periodically evaluate the transmit power for all joined access points. However, the Cisco WLC updates the power, if necessary, only when you click **Invoke Power Update Now**.

  Note The Cisco WLC does not evaluate and update the transmit power immediately after you click **Invoke Power Update Now**. It waits for the next 600-second interval. This value is not configurable.

- **Fixed**—Prevents the Cisco WLC from evaluating and, if necessary, updating the transmit power for joined access points. The power level is set to the fixed value chosen from the drop-down list.

  Note The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain, channel, and antennas in which the access points are deployed.

  Note For optimal performance, we recommend that you use the Automatic setting.

Step 4 Enter the maximum and minimum power level assignment values in the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes.

The range for the Maximum Power Level Assignment is –10 to 30 dBm.

The range for the Minimum Power Level Assignment is –10 to 30 dBm.

Step 5 In the Power Threshold text box, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter is –70 dBm for TPCv1 and –67 dBm for TPCv2, but can be changed when access points are transmitting at higher (or lower) than desired power levels.

The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at a higher transmit power. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

This page also shows the following nonconfigurable transmit power level parameter settings:

- Power Neighbor Count—The minimum number of neighbors an access point must have for the transmit power control algorithm to run.
- Power Assignment Leader—The MAC address of the RF group leader, which is responsible for power level assignment.

- Last Power Level Assignment—The last time RRM evaluated the current transmit power level assignments.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a "coverage hole" alert to the controller. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The controller discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the controller mitigates the coverage hole by increasing the transmit power level for that specific access point. The controller does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

Configuring Coverage Hole Detection (GUI)

Procedure

Step 1 Disable the 802.11 network as follows:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) **Global Parameters** page.

b) Unselect the **802.11a** (or **802.11b/g**) **Network Status** check box.

c) Click **Apply**.

Step 2 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **Coverage** to open the 802.11a/ac (or 802.11b/g/n) > RRM > Coverage page.

Step 3 Select the **Enable Coverage Hole Detection** check box to enable coverage hole detection, or unselect it to disable this feature. If you enable coverage hole detection, the Cisco WLC automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is selected.

Step 4 In the **Data RSSI** text box, enter the minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

Step 5 In the **Voice RSSI** text box, enter the minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your

network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –75 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

Step 6 In the **Min Failed Client Count per AP** text box, enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

Step 7 In the **Coverage Exception Level per AP** text box, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

Note If both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the Cisco WLC CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The Cisco WLC uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP text boxes over a 90-second period. The Cisco WLC determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Step 8 Click **Apply**.

Step 9 Reenable the 802.11 network as follows:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) **Global Parameters** page.
b) Select the **802.11a** (or **802.11b/g/n**) **Network Status** check box.
c) Click **Apply**.

Step 10 Click **Save Configuration**.

RF Profiles

RF Profiles allows you to tune groups of APs that share a common coverage zone together and selectively change how RRM will operates the APs within that coverage zone.

For example, a university might deploy a high density of APs in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and AP groups allows you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for the 802.11 radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings.

The RF profile gives you the control over the data rates and power (TPC) values.

Note The application of an RF profile does not change the AP's status in RRM. It is still in global configuration mode controlled by RRM.

To address high-density complex RF topologies, the following configurations are available:

- High Density Configurations—The following configurations are available to fine tune RF environments in a dense wireless network:
  - Client limit per WLAN or radio—Maximum number of clients that can communicate with the AP in a high-density environment.
  - Client trap threshold—Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller and Cisco Prime Infrastructure.
- Stadium Vision Configurations—You can configure the following parameter:
  - Multicast data rates—Configurable data rate for multicast traffic based on the RF condition of an AP.
- Out-of-Box AP Configurations—To create an Out-of-Box AP group that consists of newly installed access points that belong to the default AP group. When you enable this feature:
-
  - Newly installed access points (assigned to the 'default-group' AP group by default) are automatically assigned to the Out-of-Box AP group upon associating with the controller, and their radios are administratively disabled. This eliminates any RF instability caused by the new access points.
  - When Out-of-Box is enabled, default-group APs currently associated with the controller remain in the default group until they reassociate with the controller.
  - All default-group APs that subsequently associate with the controller (existing APs on the same controller that have dropped and reassociated, or APs from another controller) are placed in the Out-of-Box AP group.

Note When removing APs from the Out-of-Box AP group for production use, we recommend that you assign the APs to a custom AP group to prevent inadvertently having them revert to the Out-of-Box AP group.

  - Special RF profiles are created per 802.11 band. These RF profiles have default settings for all the existing RF parameters and additional new configurations.

Note When you disable this feature after you enable it, only subscription of new APs to the Out of Box AP group stops. All APs that are subscribed to the Out of Box AP Group remain in this AP group. The network administrators can move such APs to the default group or a custom AP group upon network convergence.

- Band Select Configurations— Band Select addresses client distribution between the 2.4-GHz and 5-GHz bands by first understanding the client capabilities to verify whether a client can associate on both 2.4-GHz

and 5-GHz spectrum. Enabling band select on a WLAN forces the AP to do probe suppression on the 2.4-GHz band that ultimately moves dual band clients to 5-GHz spectrum. You can configure the following band select parameters per AP Group:

- Probe response—Probe responses to clients that you can enable or disable.
- Probe Cycle Count—Probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
- Cycle Threshold—Time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
- Suppression Expire—Expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
- Dual Band Expire—Expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
- Client RSSI—Minimum RSSI for a client to respond to a probe.

- Load Balancing Configurations—Load balancing maintains fair distribution of clients across APs. You can configure the following parameters:
  - Window—Load balancing sets client association limits by enforcing a client window size. For example, if the window size is defined as 3, assuming fair client distribution across the floor area, then an AP should have no more than 3 clients associated with it than the group average.
  - Denial—The denial count sets the maximum number of association denials during load balancing.

- Coverage Hole Mitigation Configurations—You can configure the following parameters:
  - Data RSSI—Minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network.
  - Voice RSSI—Minimum receive signal strength indication (RSSI) value for voice packets received by the access point.
  - Coverage Exception—Percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. If an access point has more number of such clients than the configured coverage level it triggers a coverage hole event.
  - Coverage Level—Minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold to trigger a coverage hole exception.

- DCA—You can configure the following DCA parameters:
  - Avoid foreign AP interference—DCA algorithm bases its optimization on multiple sets of inputs, which include detected traffic and interference from foreign 802.11 traffic access points. Each access point periodically measures interference, noise level, foreign interference, and load and maintains a list of neighbor APs. Foreign AP interference is that which is received from 802.11 non-neighbors (i.e., 802.11 APs which are not in the same RF domain – for instance a foreign 802.11 network). This interference is measured using the same mechanism as the noise level.

Due to being out of the reach of the radio resource management module of the current deployment, such APs may be disruptive for RRM and hence the user is able to unselect their contribution to DCA in an RF profile to disable this feature.

- Channel width—You can choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n and 802.11ac radios in the 5-GHz band:
  - 20 MHz—The 20-MHz channel bandwidth (default)

Note The maximum bandwidth allowed for the 2.4-GHz band is 20 MHz.

  - 40 MHz—The 40-MHz channel bandwidth
  - 80 MHz—The 80-MHz channel bandwidth

- DCA channel list—You can choose a channel set used by DCA to assign one of the channels to an access point radio. The channel set selected for an RF profile must be a subset of the DCA global channel list. The available channels are preselected based on the globally configured countries. DCA compares the metrics measured on these channels and selects the most suitable channel. If the bandwidth is larger than 20 MHz, channel bonding takes place in sequential channels. For example, if the bandwidth is 40 MHz, the selected pair is 36 MHz and 40 MHz. For a higher bandwidth such as 80-MHz, the bandwidths selected are 36, 40, 44, and 48 MHz.
- Auto switch-over on Radar detection—With the enhancements made in DFS architecture, radar trigger on the serving channel AP will move to a new best channel that is confirmed by RRM Dynamic Channel Assignment (DCA) list. The channel width applied to such AP will also follow respective DCA channel width settings configured globally or under RF Profiles (if configured).
- Trap thresholds—The profile threshold for the traps can be configured for the specific AP groups based on the RF profiles.

Prerequisites for Configuring RF Profiles

Once you create an AP group and apply RF profiles or modify an existing AP group, the new settings are in effect and the following rules become effective:

- The same RF profile must be applied and present on every controller of the AP group or the action will fail for that controller.
- You can assign the same RF profile to more than one AP group.

Restrictions on Configuring RF Profiles

- Once you create an AP group and apply RF profiles or modify an existing AP group, the new settings are in effect and the following rules become effective:
  - AP that has a custom power setting applied for AP power is not in global mode configuration, an RF profile has no effect on this AP. For RF profiling to work, all APs must have their channel and power managed by RRM.

- Within the AP group, changing the assignment of an RF profile on either band causes the AP to reboot.
- Once you assign an RF profile to an AP group, you cannot make changes to that RF profile. You must change the AP group RF profile settings to none in order to change the RF profile and then add it back to the AP group. You can also work around this restriction by disabling the network that will be affected by the changes that you will be making either for 802.11a or 802.11b.
- You cannot delete an AP group that has APs assigned to it.
- You cannot delete an RF profile that is applied to an AP group.

- If you enable Out of Box, save the configuration, and then reboot the Cisco WLC, the status of Out of Box is changed to disabled state. This behavior is observed in Cisco WiSM2, Cisco 5508 WLC, and Cisco 2504 WLC. The workaround is to enable Out of Box again after you reboot the Cisco WLC.

Configuring an RF Profile (GUI)

Procedure

Step 1 Choose **Wireless** > **RF Profiles** to open the RF profiles page.

Step 2 To configure the out-of-box status for all RF profiles, select or unselect the **Enable Out Of Box** check box.

Step 3 Click **New**.

Step 4 Enter the RF Profile Name and choose the radio band.

Step 5 Click **Apply** to configure the customizations of power and data rate parameters.

Step 6 In the **General** tab, enter the description for the RF profile in the Description text box.

Step 7 In the **802.11** tab, configure the data rates to be applied to the APs of this profile.

Step 8 In the **RRM** tab, do the following:

a) In the TPC area, configure the Maximum and Minimum Power Level Assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use.

b) In the TPC area, configure a custom TPC power threshold for either Version1 or Version 2 of TPC.

Note Only one version of TPC can be operable for RRM on a given controller Version 1 and Version 2 are not interoperable within the same RF profile. If you select a threshold value for TPCv2 and it is not in the chosen TPC algorithm for the RF profile, this value will be ignored.

c) In the Coverage Hole Detection area, configure the voice and data RSSI.

d) In the Coverage Exception text box, enter the number for clients.

e) In the Coverage Level text box, enter the percentage.

f) In the Profile threshold for Traps area, enter the interference percentage, number of clients, noise level, and utilization percentage.

g) In the DCA area, select the Avoid Foreign AP interference **Enabled** check box to avoid foreign AP interference.

h) In the High-Speed Roam area, select the HSR mode **Enabled** check box to optimize high-speed roaming.

i) In the High-Speed Roam area, enter the neighbor timeout factor.

j) In the DCA area, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n and 802.11 ac radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)
- **40 MHz**—The 40-MHz channel bandwidth
- **80 MHz**—The 80-MHz channel bandwidth

k) In the DCA area, the **DCA Channels** field shows the channels that are currently selected. To choose a channel, check its check box in the **Select** column. To exclude a channel, uncheck its check box. The channel numbers listed are applicable only for that particular RF profile.

The RF profile channel list must be a subset of the global channel list. That is, you may not enable a channel in the RF profile that is not enabled globally.

To configure a DCA channel list, enter this command in the CLI: **config rf-profile channel** {**add** | **delete**} *chan-profile-name*

Step 9 In the **High Density** tab, do the following:

a) In the High Density Parameters area, enter the maximum number of clients to be allowed per AP radio and the client trap threshold value.

b) In the Multicast Parameters area, choose the data rates from the Multicast Data Rates drop-down list.

Step 10 In the **Client Distribution** tab, do the following:

a) In the Load Balancing area, enter the client window size and the denial count.

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.

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

b) In the Band Select area, select or unselect the **Probe Response** check box.

Note The Band Select configurations are available only for the 802.11b/g RF profiles.

c) In the Cycle Count text box, enter a value that sets the number of suppression cycles for a new client. The default count is 2.

d) In the Cycle Threshold text box, enter a time period in milliseconds that determines the time threshold during which new probe requests from a client from a new scanning cycle. The default cycle threshold is 200 milliseconds.

e) In the Suppression Expire text box, enter a time period after which the 802.11 b/g clients become new and are subject to probe response suppression.

f) In the Dual Band Expire text box, enter a time period after which the dual band clients become new and are subject to probe response suppression.

g) In the Client RSSI text box, enter the minimum RSSI for a client to respond to a probe.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring an RF Profile (CLI)

Procedure

Step 1 To configure the out-of-box status for all RF profiles, enter this command:

config rf-profile out-of-box {**enable** | **disable**}

Step 2 To create or delete an RF profile, enter this command:

config rf-profile {**create** {**802.11a** | **802.11b**} | **delete**} *profile-name*

Step 3 To specify a description for the RF profile, enter this command:

config rf-profile description *text profile-name*

Step 4 To configure the data rates to be applied to the APs of this profile, enter this command:

config rf-profile data-rates {**802.11a** | **802.11b**} {**disabled** | **mandatory** | **supported**} *rate profile-name*

Step 5 To configure the maximum and minimum power level assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use, enter this command:

config rf-profile {**tx-power-max** | **tx-power-min**} *power-value profile-name*

Step 6 To configure a custom TPC power threshold for either Version1 or Version 2 of TPC, enter this command:

config rf-profile {**tx-power-control-thresh-v1** | **tx-power-control-thresh-v2**} *power-threshold profile-name*

Step 7 To configure the coverage hole detection parameters:

a) To configure the coverage data, enter this command:

config rf-profile coverage data *value-in-dBm profile-name*

b) To configure the minimum client coverage exception level, enter this command:

config rf-profile coverage exception *clients profile-name*

c) To configure the coverage exception level percentage, enter this command:

config rf-profile coverage level *percentage-value profile-name*

d) To configure the coverage of voice, enter this command:

config rf-profile coverage voice *value-in-dBm profile-name*

Step 8 To configure the maximum number of clients to be allowed per AP radio, enter this command:

config rf-profile max-clients *num-of-clients profile-name*

Step 9 To configure the client trap threshold value, enter this command:

config rf-profile client-trap-threshold *threshold-value profile-name*

Step 10 To configure multicast, enter this command:

config rf-profile multicast data-rate *rate profile-name*

Step 11 To configure load balancing, enter this command:

config rf-profile load-balancing {**window** *num-of-clients* | **denial** *value*} *profile-name*

Step 12 To configure band select:

a) To configure the band select cycle count, enter this command:

config rf-profile band-select cycle-count *max-num-of-cycles profile-name*

b) To configure the cycle threshold, enter this command:

config rf-profile band-select cycle-threshold *time-in-milliseconds profile-name*

c) To configure the expiry of the band select, enter this command:

config rf-profile band-select expire {**dual-band** | **suppression**} *time-in-seconds profile-name*

d) To configure the probe response, enter this command:

config rf-profile band-select probe-response {**enable** | **disable**} *profile-name*

e) To configure the minimum RSSI for a client to respond to a probe, enter this command:

config rf-profile band-select client-rssi *value-in-dBm profile-name*

Step 13 Configure the 802.11n only mode for an access point group base by entering this command:

config rf-profile 11n-client-only {**enable** | **disable**} *rf-profile-name*

In the 802.11n only mode, the access point broadcasts support for 802.11n speeds. Only 802.11n clients are allowed to associate with the access point

Step 14 To configure the DCA parameters for an RF profile:

- To configure foreign AP interference, enter this command:

  config rf-profile channel foreign { **enable** | **disable** } *profile-name*

- To configure channel width, enter this command:

  config rf-profile channel foreign { **enable** | **disable** } *profile-name*

- To configure a DCA channel list, enter this command:

  config rf-profile channel { **add** | **delete** } *chan profile_name*

- To configure trap threshold, enter this command:

  config rf-profile trap-threshold { **clients** | **interference** | **noise** | **utilization** } *profile-name*

  - **clients**—The number of clients on an access point's radio for the trap is between 1 and 200. The default is 12.
  - **interference**—The percentage of interference threshold for the trap is from 0 to 100 percent. The default is 10 percent.
  - **noise**—The noise threshold for the trap is from -127 to 0 dBm. The default is -17 dBm.

- **utilization**—The percentage of bandwidth being used by an access-point threshold for the trap is from 0 to 100 percent. The default is 80 percent.

Applying an RF Profile to AP Groups (GUI)

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.

Step 2 Click the AP Group Name to open the AP Group > Edit page.

Step 3 Click the **RF Profile** tab to configure the RF profile details. You can choose an RF profile for each band (802.11a/802.11b) or you can choose just one or none to apply to this group.

Note Until you choose the APs and add them to the new group, no configurations are applied. You can save the new configuration as is, but no profiles are applied. Once you choose the APs to move the AP group, the process of moving the APs into the new group reboots the APs and the configurations for the RF profiles are applied to the APs in that AP group.

Step 4 Click the **APs** tab and choose the APs to add to the AP group.

Step 5 Click **Add APs** to add the selected APs to the AP group. A warning message displays that the AP group will reboot the APs will rejoin the controller.

Note APs cannot belong to two AP groups at once.

Step 6 Click **Apply**. The APs are added to the AP Group.

Applying RF Profiles to AP Groups (CLI)

Procedure

Apply RF profiles to AP groups by entering this command:

config wlan apgroup profile-mapping {**add** | **delete**} *ap-group-name rf-profile-name*

Debug RRM Issues (CLI)

Procedure

Use these commands to troubleshoot and verify RRM behavior:

debug airewave-director *?*

where *?* is one of the following:

- **all**—Enables debugging for all RRM logs.
- **channel**—Enables debugging for the RRM channel assignment protocol.
- **detail**—Enables debugging for RRM detail logs.
- **error**—Enables debugging for RRM error logs.
- **group**—Enables debugging for the RRM grouping protocol.
- **manager**—Enables debugging for the RRM manager.
- **message**—Enables debugging for RRM messages.
- **packet**—Enables debugging for RRM packets.
- **power**—Enables debugging for the RRM power assignment protocol as well as coverage hole detection.
- **profile**—Enables debugging for RRM profile events.
- **radar**—Enables debugging for the RRM radar detection/avoidance protocol.
- **rf-change**—Enables debugging for RRM RF changes.

CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all of the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act upon this information. For example, you could manually remove the interfering device, or the system could automatically change the channel away from the interference. CleanAir provides spectrum management and RF visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points, Cisco Wireless LAN Controllers, and Cisco Prime Infrastructure. These access points collect information about all devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the controller. The controller controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or Cisco Connected Mobile Experiences (CMX) upon request.

For every device operating in the unlicensed band, Cisco CleanAir tells you what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert.

Wireless LAN systems operate in unlicensed 2.4- and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect Wi-Fi operations.

Some of the most advanced WLAN services, such as voice over wireless and IEEE 802.11n radio communications, could be significantly impaired by the interference caused by other legal users of the ISM

bands. The integration of Cisco CleanAir functionality into the Cisco Unified Wireless Network addresses this problem of radio frequency (RF) interference.

CleanAir is supported on mesh AP backhaul at a 5-GHz radio of mesh. You can enable CleanAir on backhaul radios and can provide report interference details and air quality.

This section contains the following subsections:

Role of the Cisco Wireless LAN Controller in a Cisco CleanAir System

The controller performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI, CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data
- Displays spectrum data.
- Collects and processes air quality reports from the access point and stores them in the air quality database. The Air Quality Report (AQR) contains information about the total interference from all identified sources represented by the Air Quality Index (AQI) and summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per interference type reports, which enables you to take action in cases where the interference due to unclassified interfering devices is more.
- Collects and processes interference device reports (IDRs) from the access point and stores them in the interference device database.
- Forwards spectrum data to Cisco Prime Infrastructure and Cisco CMX.

Interference Types that Cisco CleanAir Can Detect

Cisco CleanAir can detect interference, report on the location and severity of the interference, and recommend different mitigation strategies. Two such mitigation strategies are persistent device avoidance and spectrum event-driven RRM.

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its location and potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. For CleanAir, two types of interference events are common:

- Persistent interference
- Spontaneous interference

Persistent interference events are created by devices that are stationary in nature and have intermittent but largely repeatable patterns of interference. For example, consider the case of a microwave oven located in a break room. Such a device might be active for only 1 or 2 minutes at a time. When operating, however, it can be disruptive to the performance of the wireless network and associated clients. Using Cisco CleanAir, you can positively identify the device as a microwave oven rather than indiscriminate noise. You can also determine exactly which part of the band is affected by the device, and because you can locate it, you can understand which access points are most severely affected. You can then use this information to direct RRM in selecting a channel plan that avoids this source of interference for the access points within its range. Because this interference is not active for a large portion of the day, existing RF management applications might attempt to again change the channels of the affected access points. Persistent device avoidance is unique, however, in that it remains in effect as long as the source of interference is periodically detected to refresh the persistent status. The Cisco CleanAir system knows that the microwave oven exists and includes it in all future planning. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interferences only if the devices are actively transmitting. Bluetooth devices have extensive power save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

Persistent Devices

Some interference devices such as outdoor bridges and microwave ovens only transmit when needed. These devices can cause significant interference to the local WLAN due to short duration and periodic operation remain largely undetected by normal RF management metrics. With CleanAir the RRM DCA algorithm can detect, measure, register and remember the impact and adjust the DCA algorithm. This minimizes the use of channels affected by the persistent devices in the channel plan local to the interference source. Cisco CleanAir detects and stores the persistent device information in the controller and this information is used to mitigate interfering channels.

Persistent Device Awareness (PDA)

This relies on detection by a CleanAir AP. The neighbors of the detecting AP can have the PDA information shared through RRM and the channel information biased to help a non-CleanAir AP avoid the interference for a given channel.

Persistent Devices Detection

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and stores the information in the Cisco WLC. Local/Bridge mode AP detects interference devices on the serving channels only.

Persistent Devices Propagation

Persistent device information that is detected by local or monitor mode access points is propagated to the neighboring access points connected to the same Cisco WLC to provide better chance of handling and avoiding persistent devices. Persistent device detected by the CleanAir-enabled access point is propagated to neighboring non-CleanAir access points, thus enhancing channel selection quality.

Detecting Interferers by an Access Point

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed which results in the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device detection history is preserved.

For example, some Bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Detecting Persistent Sources of Interference

Procedure

See a list of persistent sources of interference for a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show ap auto-rf {**802.11a** | **802.11b**} *Cisco_AP*

Prerequisites for CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only. An AP can only measure air quality and interference when the AP is not busy transmitting Wi-Fi frames. This implies that CleanAir detections will be drastically lower if the AP is having a high channel utilization.
- FlexConnect—When a FlexConnect access point is connected to the controller , its Cisco CleanAir functionality is identical to local mode.
- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

The following options are available:

- All—All channels
- DCA—Channel selection governed by the DCA list
- Country—All channels are legal within a regulatory domain

- SE-Connect—This mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, bypassing the controller. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the controller. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only. Up to three active Spectrum Expert connections are possible.

Restrictions for CleanAir

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the controller's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- Spectrum Expert (SE) Connect functionality is supported for local, FlexConnect, bridge, and monitor modes. The access point provides spectrum information to Spectrum Expert only for the current channel(s). For local, FlexConnect, and bridge modes, the spectrum data is available for the current active channel(s) and for the monitor mode, the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the controller and perform normal activities according to the current mode. Sniffer and rogue detections access point modes are incompatible with all types of CleanAir spectrum monitoring.
- For 4800 AP slot 1 5 GHz is dedicated and cannot be individually moved to monitor mode. However, slot 0 is XOR and can be moved to monitor as well as 2.4/5 GHz. Slot 2 is dedicated monitor and will operate in 5GHz and in AP monitor mode, slot 2 will be disabled because a monitor radio is already available in both 2.4/5GHz. 3700 AP has dedicated 2.4GHz (slot0) and 5GHz (slot1).
- Do not connect access points in SE connect mode directly to any physical port on the controller.
- CleanAir is not supported wherein the channel width is 160 MHz.

Configuring Cisco CleanAir on the Controller

Configuring Cisco CleanAir on Cisco WLC (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac or 802.11b/g/n > CleanAir** to open the **802.11a (or 802.11b) > CleanAir** page.

Step 2 Check the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or uncheck it to prevent the Cisco WLC from detecting spectrum interference. By default, this feature is in disabled state.

Step 3 Check the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or uncheck it to prevent the Cisco WLC from reporting interferers. By default, this feature is in enabled state.

Note Device Security alarms, Event Driven RRM, and the Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.

Step 4 Check the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring APs connected to the same Cisco WLC. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5 Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the **Interferences to Detect** box and any that do not need to be detected appear in the **Interferences to Ignore** box. By default, all interference sources are detected. The possible sources of interference that you can choose are as follows:

- **Bluetooth Paging Inquiry**—A Bluetooth discovery (802.11b/g/n only)
- **Bluetooth Sco Acl**—A Bluetooth link (802.11b/g/n only)
- **Generic DECT**—A digital enhanced cordless communication (DECT)-compatible phone
- **Generic TDD**—A time division duplex (TDD) transmitter
- **Generic Waveform**—A continuous transmitter
- **Jammer**—A jamming device
- **Microwave—**A microwave oven (802.11b/g/n only)
- **Canopy**—A canopy bridge device
- **Spectrum 802.11 FH—**An 802.11 frequency-hopping device (802.11b/g/n only)
- **Spectrum 802.11 inverted**—A device using spectrally inverted Wi-Fi signals
- **Spectrum 802.11 non std channel**—A device using nonstandard Wi-Fi channels
- **Spectrum 802.11 SuperG**—An 802.11 SuperAG device
- **Spectrum 802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **Video Camera**—An analog video camera
- **WiMAX Fixed**—A WiMAX fixed device (802.11a/n/ac only)
- **WiMAX Mobile**—A WiMAX mobile device (802.11a/n/ac only)
- **XBox**—A Microsoft Xbox (802.11b/g/n only)

Note When you include BLE Beacon in the **Interferences to Detect** list, the 2.4GHz serving radio periodically goes off channel for a scan.

Note APs that are associated to the Cisco WLC send interference reports only for the interferers that appear in the **Interferences to Detect** box. This functionality allows you to filter out interferers that you do not want as well as any that may be flooding the network and causing performance problems for the Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 6 Configure Cisco CleanAir alarms as follows:

a) Check the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or uncheck the box to disable this feature. By default, this feature is in enabled state.

b) If you checked the **Enable AQI Trap** check box in *Step a*, enter a value between 1 and 100 (inclusive) in the **AQI Alarm Threshold** field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

c) Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality reaches a threshold value. The default is 35. Valid range is from 1 and 100.

d) Check the **Enable trap for Unclassified Interferences** check box to enable the AQI alarm to be generated upon detection of unclassified interference beyond the severity threshold specified in the **AQI Alarm Threshold** field. Unclassified interferences are interferences that are detected but do not correspond to any of the identifiable interference types.

e) Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value from 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

f) Check the **Enable Interference Type Trap** check box to trigger interferer alarms when the Cisco WLC detects specified device types, or uncheck it to disable this feature. By default, this feature is in enabled state.

g) Ensure that any sources of interference that need to trigger interferer alarms appear in the **Trap on These Types** box and any that do not need to trigger interferer alarms appear in the **Do Not Trap on These Types** box. By default, all interference sources trigger interferer alarms.

   For example, if you want the Cisco WLC to send an alarm when it detects a jamming device, check the **Enable Interference Type Trap** check box and move the jamming device to the **Trap on These Types** box.

Step 7 Click **Apply**.

Step 8 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled AP detects a significant level of interference as follows:

a) Look at the **EDRRM** field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b) If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page is displayed.

c) Check the **EDRRM** check box to trigger RRM to run when an AP detects a certain level of interference, or uncheck it to disable this feature. By default, this feature is in enabled state.

d) If you checked the **EDRRM** check box in *Step c*, choose **Low**, **Medium**, **High,** or **Custom** from the **Sensitivity Threshold** drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the AP rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected AP radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

   If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

   The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

e) To configure rogue duty cycle, check the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in terms of percentage. The default value of **Rogue Duty-Cycle** is 80%.

f) Save the configuration.

Configuring Cisco CleanAir on Cisco WLC (CLI)

Procedure

Step 1 Configure Cisco CleanAir functionality on the 802.11 network by entering this command:

config {**802.11a** | **802.11b**} **cleanair** {**enable** | **disable**} *all*

If you disable this feature, the Cisco WLC does not receive any spectrum data. By default, this feature is in disabled state.

Step 2 Enable CleanAir on all associated access points in a network:

config {**802.11a** | **802.11b**} **cleanair enable network**

You can enable CleanAir on a 5-GHz radio of mesh access points.

Step 3 Configure interference detection and specify sources of interference that need to be detected by the Cisco CleanAir system by entering this command:

config {**802.11a** | **802.11b**} **cleanair device** {**enable** | **disable**} *type*

where you choose the *type* as one of the following:

- **802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A Bluetooth discovery (802.11b/g/n only)
- **bt-link**—A Bluetooth link (802.11b/g/n only)
- **canopy**—A canopy device
- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A microwave oven (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video camera**—An analog video camera
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)

Note Access points that are associated to the Cisco WLC send interference reports only for the interference types specified in this command. This functionality allows you to filter out interferers that may be flooding the network and causing performance problems for the Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 4 Configure the triggering of air quality alarms by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm air-quality** {**enable** | **disable**}

The default value is enabled.

Step 5 Specify the threshold at which you want the air quality alarm to be triggered by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm air-quality threshold** *threshold*

where *threshold* is a value between 1 and 100 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 6 Enable the triggering of interferer alarms by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm device** {**enable** | **disable**}

The default value is enable.

Step 7 Specify sources of interference that trigger alarms by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm device** *type* {**enable** | **disable**}

where you choose the *type* as one of the following:

- **802.11-fh—**An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A Bluetooth discovery (802.11b/g/n only)
- **bt-link**—A Bluetooth link (802.11b/g/n only)
- **canopy**—A canopy device
- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A microwave oven (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video camera**—An analog video camera
- wimax-fixed—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)

Step 8 Configure the triggering of air quality alarms for unclassified devices by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm unclassified** {**enable** | **disable**}

Step 9 Specify the threshold at which you want the air quality alarm to be triggered for unclassified devices by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm unclassified threshold** *threshold*

where *threshold* is a value from 1 and 99 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 10 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

config advanced {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}—Enables or disables spectrum event-driven RRM. The default value is disabled.

config advanced {**802.11a** | **802.11b**} **channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Specifies the threshold at which you want RRM to be triggered. When the interference level for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while high represents an increased sensitivity. You can also set the sensitivity to a custom level of your choice. The default value is medium.

config advanced {**802.11a** | **802.11b**} **channel cleanair-event sensitivity threshold** *thresholdvalue*—If you set the threshold sensitivity as custom, you must set a custom threshold value. The default is 35.

Step 11 Configure and monitor Interference Awareness by entering the following commands:

- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution duty-cycle** *value*
- **show** {**802.11a** | **802.11b**} **cleanair config**
- **debug airewave-director profile enable**
- **debug airewave-director channel enable**

Step 12 Enable persistent devices propagation by entering this command:

config advanced {**802.11a** | **802.11b**} **channel pda-prop** {**enable** | **disable**}

Step 13 Save your changes by entering this command:

save config

Step 14 See the Cisco CleanAir configuration for the 802.11a/n or 802.11b/g/n network by entering this command:

show {**802.11a** | **802.11b**} **cleanair config**

Information similar to the following appears:

```
(Cisco Controller) >show 802.11a cleanair config

Clean Air Solution................................ Disabled
Air Quality Settings:
    Air Quality Reporting......................... Enabled
    Air Quality Reporting Period (min)............ 15
    Air Quality Alarms............................ Enabled
      Air Quality Alarm Threshold................. 35
      Unclassified Interference................... Disabled
      Unclassified Severity Threshold............. 20
Interference Device Settings:
    Interference Device Reporting................. Enabled
    Interference Device Types:
        TDD Transmitter........................... Enabled
```

```
        Jammer.................................. Enabled
        Continuous Transmitter.................. Enabled
        DECT-like Phone......................... Enabled
        Video Camera............................ Enabled
        WiFi Inverted........................... Enabled
        WiFi Invalid Channel.................... Enabled
        SuperAG................................. Enabled
        Canopy.................................. Enabled
        WiMax Mobile............................ Enabled
  WiMax Fixed.............................. Enabled
Interference Device Alarms................... Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter......................... Disabled
        Jammer.................................. Enabled
        Continuous Transmitter.................. Disabled
        DECT-like Phone......................... Disabled
        Video Camera............................ Disabled
        WiFi Inverted........................... Enabled
        WiFi Invalid Channel.................... Enabled
        SuperAG................................. Disabled
        Canopy.................................. Disabled
        WiMax Mobile............................ Disabled
        WiMax Fixed............................. Disabled
Additional Clean Air Settings:
    CleanAir ED-RRM State....................... Disabled
    CleanAir ED-RRM Sensitivity................. Medium
    CleanAir ED-RRM Custom Threshold............ 50
    CleanAir Persistent Devices state........... Disabled
    CleanAir Persistent Device Propagation...... Enabled
```

Step 15 See the spectrum event-driven RRM configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:

show advanced {**802.11a** | **802.11b**} *channel*

Information similar to the following appears:

```
Automatic Channel Assignment
  Channel Assignment Mode..................... AUTO
  Channel Update Interval..................... 600 seconds [startup]
  Anchor time (Hour of the day)............... 0
  Channel Update Contribution................. SNI
  CleanAir Event-driven RRM option............ Enabled
CleanAir Event-driven RRM sensitivity...... Medium
```

Configuring Cisco CleanAir on an Access Point

Configuring Cisco CleanAir on an Access Point (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points > Radios > 802.11a/n/ac or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 2 Hover your cursor over the blue drop-down arrow for the desired access point and click **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page appears.

The **CleanAir Capable** field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

Step 3 Enable Cisco CleanAir functionality for this access point by choosing **Enable** from the CleanAir Status drop-down list. To disable CleanAir functionality for this access point, choose **Disable**. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

The **Number of Spectrum Expert Connections** text box shows the number of Spectrum Expert applications that are currently connected to the access point radio. Up to three active connections are possible.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 Click **Back** to return to the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 7 View the Cisco CleanAir status for each access point radio by looking at the **CleanAir Status** text box on the 802.11a/n/ac (or 802.11b/g/n) Radios page.

The Cisco CleanAir status is one of the following:

- **UP**—The spectrum sensor for the access point radio is currently operational (error code 0).
- **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.
- **ERROR**—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.
- **N/A**—This access point radio is not capable of supporting Cisco CleanAir functionality.

Note You can create a filter to make the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific Cisco CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP dialog box, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).

Configuring Cisco CleanAir on an Access Point (CLI)

Procedure

Step 1 Configure Cisco CleanAir functionality for a specific access point by entering this command:

config {**802.11a** | **802.11b**} **cleanair {enable | disable}***Cisco_AP*

Step 2 Save your changes by entering this command:

save config

Step 3 See the Cisco CleanAir configuration for a specific access point on the 802.11a/n/ac/ac or 802.11b/g/n/ac network by entering this command:

show ap config {802.11a | 802.11b} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Disabled
   Spectrum Sensor State................. Configured (Error code = 0)
```

Monitoring Interference Devices

Prerequisites for Monitoring the Interference Devices

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Monitoring the Interference Device (GUI)

Procedure

Step 1 Choose **Monitor > Cisco CleanAir > 802.11a/n or 802.11b/g/n > Interference Devices** to open the CleanAir > Interference Devices page.

This page shows the following information:

- **AP Name**—The name of the access point where the interference device is detected.
- **Radio Slot #**—Slot where the radio is installed.
- **Interferer Type**—Type of the interferer.
- **Affected Channel**—Channel that the device affects.
- **Detected Time**—Time at which the interference was detected.
- **Severity**—Severity index of the interfering device.
- **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
- **RSSI**—Receive signal strength indicator (RSSI) of the access point.
- **DevID**—Device identification number that uniquely identified the interfering device.

- **ClusterID**—Cluster identification number that uniquely identifies the type of the devices.

Step 2 Click **Change Filter** to display the information about interference devices based on a particular criteria.

Step 3 Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of interference devices that are based on the following filtering parameters:

- **Cluster ID**—To filter based on the Cluster ID, select the check box and enter the Cluster ID in the text box next to this field.
- **AP Name**—To filter based on the access point name, select the check box and enter the access point name in the text box next to this field.
- **Interferer Type**—To filter based on the type of the interference device, select the check box and select the interferer device from the options.

  Select one of the interferer devices:

  - **BT Link**
  - **MW Oven**
  - **802.11 FH**
  - **BT Discovery**
  - **TDD Transmit**
  - **Jammer**
  - **Continuous TX**
  - **DECT Phone**
  - **Video Camera**
  - **802.15.4**
  - **WiFi Inverted**
  - **WiFi Inv. Ch**
  - **SuperAG**
  - **Canopy**
  - **XBox**
  - **WiMax Mobile**
  - **WiMax Fixed**
  - **WiFi ACI**
  - **Unclassified**

- **Activity Channels**
- **Severity**

- **Duty Cycle (%)**
- **RSSI**

Step 4 Click **Find**.

The current filter parameters are displayed in the Current Filter field.

Monitoring the Interference Device (CLI)

Detecting Interferers by an Access Point

Procedure

See information for all of the interferers detected by a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair device ap** *Cisco_AP*

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed which results in the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device detection history is preserved.

For example, some Bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Detecting Interferers by Device Type

Procedure

See information for all of the interferers of a specific device type on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair device type** *type*

where you choose *type* as one of the following:

- **802.11a**
  - **802.11-inv**—A device using spectrally inverted Wi-Fi signals

- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **canopy**—A canopy bridge device
- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video**—A video device
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device

- **802.11b**
  - **bt-link**—A Bluetooth link device
  - **bt-discovery**—A Bluetooth discovery device
  - **ble-beacon**—A BLE beacon device
  - **mw-oven—**A microwave oven device
  - **802.11-fh—**An 802.11 frequency-hopping device
  - **802.15.4**—An 802.15.4 device
  - **tdd-tx**—A time division duplex (TDD) transmitter
  - **jammer**—A jamming device
  - **cont-tx**—A continuous transmitter
  - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
  - **video**—A video device
  - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
  - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
  - **superag**—An 802.11 SuperAG device
  - **canopy**—A canopy bridge device
  - **wimax-mobile**—A WiMAX mobile device
  - **wimax-fixed**—A WiMAX fixed device
  - **msft-xbox**—A Microsoft Xbox device

Note No more than 25 interferers can be detected by a Cisco AP.

Monitoring Persistent Devices (GUI)

Procedure

Choose **Wireless** > **Access Points > Radios > 802.11a/n/ac or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page. Hover your cursor over the blue drop-down arrow for the desired access point and click **Detail**. The 802.11a/n/ac (or 802.11b/g/n) AP Interfaces > Detail page is displayed.

This page displays the details of the access points along with the list of persistent devices detected by this access point. Details of the persistent devices is displayed under the Persistent Devices section.

The following information for each persistent device is available:

- Class Type—The class type of the persistent device.
- Channel—Channel this device is affecting.
- DC(%)—Duty cycle (in percentage) of the persistent device.
- RSSI(dBm)—RSSI indicator of the persistent device.
- Last Seen Time—Timestamp when the device was last active.

Monitoring Persistent Devices (CLI)

Procedure

To view the list of persistent devices using the CLI, use the following command:

show ap auto-rf {**802.11a** | **802.11b**} *ap_name*

Information similar to the following appears:

```
Number Of Slots.................................. 2
AP Name.......................................... AP_1572_MAP
MAC Address...................................... c4:7d:4f:3a:35:38
  Slot ID........................................ 1
  Radio Type..................................... RADIO_TYPE_80211a
  Sub-band Type.................................. All
  Noise Information
. . ..
. . . .
Power Level.................................. 1
    RTS/CTS Threshold.......................... 2347
    Fragmentation Threshold.................... 2346
    Antenna Pattern............................ 0

Persistent Interference Devices
  Class Type   Channel  DC (%%)  RSSI (dBm)  Last Update Time
  -----------  -------  ------  ----------  ------------------------
  Video Camera   149      100     -34        Tue Nov 8 10:06:25 2020
```

The following information for each persistent device is available:

- Class Type—The class type of the persistent device.
- Channel—Channel this device is affecting.
- DC(%)—Duty cycle (in percentage) of the persistent device.
- RSSI(dBm)—RSSI indicator of the persistent device.
- Last Seen Time—Timestamp when the device was last active.

Monitoring the Air Quality of Radio Bands

This section describes how to monitor the air quality of the 802.11a/n/ac and 802.11b/g/n radio bands using both the controller GUI and CLI.

Monitoring the Air Quality of Radio Bands (GUI)

Procedure

Choose **Monitor > Cisco CleanAir > 802.11a/n/ac or 802.11b/g/n >Air Quality Report** to open the **CleanAir > Air Quality Report** page.

This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. Specifically, it shows the following information:

- AP Name: The name of the access point that reported the worst air quality for the 802.11a/n/ac or 802.11b/g/n radio band.
- Radio Slot: The slot number where the radio is installed.
- Channel: The radio channel where the air quality is monitored.
- Minimum AQ: The minimum air quality for this radio channel.
- Average AQ: The average air quality for this radio channel.
- Interferer: The number of interferers detected by the radios on the 802.11a/n/ac or 802.11b/g/n radio band.
- DFS: Dynamic Frequency Selection. This indicates if DFS is enabled or not.

Monitoring the Air Quality of Radio Bands (CLI)

Viewing a Summary of the Air Quality

Procedure

See a summary of the air quality for the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality summary**

Viewing Air Quality for all Access Points on a Radio Band

Procedure

See information for the 802.11a/n/ac or 802.11b/g/n access point with the air quality by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality**

Viewing Air Quality for an Access Point on a Radio Band (CLI)

Procedure

See air quality information for a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality** *Cisco_AP*

Monitoring the Worst Air Quality of Radio Bands (GUI)

Procedure

Step 1 Choose **Monitor** > **Cisco CleanAir** >**Worst Air-Quality** to open the **CleanAir > Worst Air Quality Report** page.

This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. Specifically, it shows the following information:

- **AP Name**—The name of the access point that reported the worst air quality for the 802.11 radio band.
- **Channel Number**—The radio channel with the worst reported air quality.
- **Minimum Air Quality Index(1 to 100)**—The minimum air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index(1 to 100)**—The average air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—The number of interferers detected by the radios on the 802.11 radio band.

Step 2 See a list of persistent sources of interference for a specific access point radio as follows:

a) **Choose Wireless** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

b) Hover your cursor over the blue drop-down arrow for the desired access point radio and click **CleanAir-RRM**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > *Access Point Name* > Persistent Devices page appears. This page lists the device types of persistent sources of interference detected by this access point radio. It also shows the channel on which the interference was detected, the percentage of time that the interferer was active (duty cycle), the received signal strength (RSSI) of the interferer, and the day and time when the interferer was last detected.

Monitoring the Worst Air Quality of Radio Bands (CLI)

This section describes the commands that you can use to monitor the air quality of the 802.11 radio band.

Viewing a Summary of the Air Quality (CLI)

See a summary of the air quality for the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality summary**

Viewing the Worst Air Quality Information for all Access Points on a Radio Band (CLI)

See information for the 802.11a/n/ac or 802.11b/g/n access point with the worst air quality by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality worst**

Viewing the Air Quality for an Access Point on a Radio Band (CLI)

See the air quality information for a specific access point on the 802.11 radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality** *Cisco_AP*

Viewing the Air Quality for an Access Point by Device Type (CLI)

- See information for all of the interferers detected by a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

  show {802.11a | 802.11b} cleanair device ap *Cisco_AP*

- See information for all of the interferers of a specific device type on the 802.11a/n or 802.11b/g/n radio band by entering this command:

  show {802.11a | 802.11b} cleanair device type *type*

  where you choose *type* as one of the following:

  - **802.11a**
    - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
    - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
    - **canopy**—A canopy bridge device
    - **cont-tx**—A continuous transmitter
    - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
    - **jammer**—A jamming device
    - **superag**—An 802.11 SuperAG device

- **tdd-tx**—A time division duplex (TDD) transmitter
- **video**—A video device
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device

- **802.11b**
  - **bt-link**—A Bluetooth link device
  - **bt-discovery**—A Bluetooth discovery device
  - **ble-beacon**—A BLE beacon device
  - **mw-oven—**A microwave oven device
  - **802.11-fh—**An 802.11 frequency-hopping device
  - **802.15.4**—An 802.15.4 device
  - **tdd-tx**—A time division duplex (TDD) transmitter
  - **jammer**—A jamming device
  - **cont-tx**—A continuous transmitter
  - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
  - **video**—A video device
  - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
  - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
  - **superag**—An 802.11 SuperAG device
  - **canopy**—A canopy bridge device
  - **wimax-mobile**—A WiMAX mobile device
  - **wimax-fixed**—A WiMAX fixed device
  - **msft-xbox**—A Microsoft Xbox device

Detecting Persistent Sources of Interference (CLI)

See a list of persistent sources of interference for a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show ap auto-rf {**802.11a** | **802.11b**} *Cisco_AP*