Configuring Radio Resource Management

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Radio Resource Management

The device should be configured as a mobility controller and not a mobility anchor to configure Radio Resource Management. It may require dynamic channel assignment functionality for the home APs to be supported.

The new mobility architecture that involves mobility controller and mobility agent must be configured on the switch or controllers for RRM to work.

Note Refer Mobility Configuration Guide for configuring mobility controller and mobility agent.

Restrictions for Radio Resource Management

If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.

To enable Airtime Fairness mode for APs, you should disable enforce-policy mode and reapply it again. This will change the airtime fairness configuration for all the APs. You can also use the **ap name <ap-name> dot11 24ghz airtime-fairness mode enforce-policy** command to change airtime fairness mode for individual APs.

Information About Radio Resource Management

The Radio Resource Management (RRM) software embedded in the device acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables devices 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.

RRM performs these functions:

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

Note RRM grouping will not happen, since AP operates in a static channel which is not in the DCA channel list. NDP is sent only on DCA channels and when radio operates on a non-DCA channel it will not receive NDA on-channel.

Radio Resource Monitoring

RRM automatically detects and configures new devices 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 scan all valid channels for the country of operation as well as for channels available in other locations. The access points in local mode 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.

Note In the presence of voice traffic or other critical traffic (in the last 100 ms), the access points can defer off-channel measurements. It also defers based on WLAN scan defer priority configurations.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

RRM supports new mobility architecture for RF grouping that involves Mobility Controller (MC) and Mobility Agent (MA).

- Mobility Controller (MC)—The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.
- Mobility Agent (MA)—The Mobility Agent is the component that maintains client mobility state machine for a mobile client.

Information About RF Groups

An RF group is a logical collection of Cisco WLCs that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering Cisco WLCs into a single RF group enable the RRM algorithms to scale beyond the capabilities of a single Cisco WLC.

RF group is created based on following parameters:

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

RF grouping runs between MCs.

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

When access points on different Cisco WLCs hear validated neighbor messages at a signal strength of –80 dBm or stronger, the Cisco WLCs 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. To know more about RF Group modes, RF Group Leader.

Note RF groups and mobility groups are similar in that they both define clusters of Cisco WLCs, 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 Cisco WLC redundancy.

RF Group Leader

Starting in the 7.0.116.0 release, the RF Group Leader can be configured in two ways as follows:

- Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a “master” 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 if RF group members experience major changes).
- Static Mode—In this mode, the user selects a Cisco WLC as an RF group leader manually. In this mode, the leader and the members are manually configured and are therefore 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 1 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 Cisco WLCs in the RF group. The RRM algorithms ensure system-wide stability and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

In Cisco WLC software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to Cisco WLCs in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. The worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio’s channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors’ neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings, if all the access point radios belong to the same RF group. This change results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and that any potential channel plan changes are controlled by the RF circumstances of a single radio. In Cisco WLC software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- Multiple local searches—The DCA search algorithm performs multiple local searches initiated by different radios within the same DCA run rather than performing a single global search driven by a single radio. This change addresses both pinning and cascading while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.
- Multiple channel plan change initiators (CPCIs)—Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio within the RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.
- Limiting the propagation of channel plan changes (Localization)—For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point,

and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.

- Non-RSSI-based cumulative cost metric—A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all access points in that area are considered in order to provide an overall understanding of the channel plan's quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves but at the expense of multiple other radios experiencing a considerable performance decline.

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 Group Name

A Cisco WLC is configured with an RF group name, which is sent to all access points joined to the Cisco WLC 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 Cisco WLCs to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a Cisco WLC may hear RF transmissions from an access point on a different Cisco WLC, you should configure the Cisco WLCs 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.

Mobility Controller

An MC can either be a group leader or a group member. One of the MCs can act as a RF group leader based on RF grouping and RF group election with other MCs. The order of priority to elect the RF leader is based on the maximum number of APs the controller or switch can support. The highest priority being 1 and the least being 5.

1. WiSM 2 Controllers
2. Cisco WLC 5700 Series Controllers
3. WiSM 1 Controllers
4. Catalyst 3850 Series Switches
5. Catalyst 3650 Series Switches

When one of the MCs becomes the RRM group leader, the remaining MCs become RRM group members. RRM group members send their RF information to the Group Leader. The group leader determines a channel and Tx power plan for the network and passes the information back to the RF group members. The MCs push the power plan to MA for the radios that belong to MA. These channel and power plans are ultimately pushed down to individual radios.

Note MC has MA functionality within it.

Mobility Agent

The MA communicates with the MC. The MC includes MAC or IP address of the switch/controller while communicating with the MA.

The MA provides the following information when polled by the MC:

- Interference or noise data.
- Neighbor data.
- Radio capabilities (supported channels, power levels).
- Radio configuration (power, channel, channel width).
- Radar data.

The MC exchanges the following information with the switch/controller (MA). The message includes:

- Configurations (channel/power/channel width) for individual radios.
- Polling requests for current configurations and RF measurements for individual radios
- Group Leader Update

In turn, the MA communicates the following messages with the MC:

- RF measurements from radios (e.g. load, noise and neighbor information)
- RF capabilities and configurations of individual radios

The MA sets channel, power, and channel width on the radios when directed by the MC. The DFS, coverage hole detection/mitigation, static channel/power configurations are performed by the MA.

Information About Rogue Access Point Detection in RF Groups

After you have created an RF group of Cisco WLCs, you need to configure the access points connected to the Cisco WLCs to detect rogue access points. The access points will then select the beacon/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 select 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 Cisco WLC.

Transmit Power Control

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

The Transmit Power Control (TPC) algorithm both 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 surrounding access points. This feature is different from

coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

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 access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out 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 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 text boxes in the Tx Power Control page. 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 device 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, then no access point would transmit above 11 dBm, unless the access point is configured manually.

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 e-mail in a café affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Devices can dynamically allocate access point channel assignments to avoid conflict and to 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 device’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 both simultaneously use 11/54 Mbps. By effectively reassigning channels, the device keeps adjacent channels separated.

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

The device 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 device 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 part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all 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 device. Using the RRM algorithms, the device 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 device 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 device may choose to avoid this channel. In very dense deployments in which all nonoverlapping channels are occupied, the device 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 device can then assign channels to improve the access point with the worst performance reported. The load is taken into account when changing the channel structure to minimize the impact on clients 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 parameter is disabled by default.

The device 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 or 80MHz channels are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

- In a single-device environment, the RRM startup mode is invoked after the device is upgraded and rebooted.
- In a multiple-device environment, the RRM startup mode is invoked after an RF Group leader is elected.

You can trigger RRM startup mode from CLI.

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 one hour, but DCA algorithm always runs in default interval of 10min, channel allocation happens for every 10min interval for the first 10 cycles, and channel changes as per DCA algorithm for every 10min. After that it goes back to the configured time interval. This is common for both DCA interval and Anchor time since it follows the steady state.

Note If DCA/TPC is turned off on the RF-group member, and auto is set on RF-group leader, the channel/TX power on member gets changed as per the algorithm run on the RF-group leader.

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 device. 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 device discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the device mitigates the coverage hole by increasing the transmit power level for that specific access point. The device 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.

How to Configure RRM

Configuring Advanced RRM CCX Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval* **Example:** `Device(config)# ap dot11 24ghz rrm ccx location-measurement 15`	Configures the interval for 802.11 CCX client location measurements. The range is from 10 to 32400 seconds.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Neighbor Discovery Type (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
	Example:
	`Device(config)#ap dot11 24ghz rrm ndp-type protected`
	`Device(config)#ap dot11 24ghz rrm ndp-type transparent`
		Configures the neighbor discovery type. By default, the mode is set to "transparent".
		• **protected**—Sets the neighbor discover type to protected. Packets are encrypted.
		• **transparent**—Sets the neighbor discover type to transparent. Packets are sent as is.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

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 Cisco WLCs 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.

Note In Auto mode , RF group leader will skip TPC and DCA for first three runs of grouping cycle in order to stabilize the RF-group

Configuring RF Group Selection Mode (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm group-mode**{**auto | leader | off**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz	5ghz rrm group-mode**{**auto	leader	off**} **Example:** `Device(config)#ap dot11 24ghz rrm group-mode leader`	Configures RF group selection mode for 802.11 bands. • **auto**—Sets the 802.11 RF group selection to automatic update mode. • **leader**—Sets the 802.11 RF group selection to leader mode. • **off**—Disables the 802.11 RF group selection.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Group Name (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wireless rf-network** *name*
3. **end**
4. **show network profile** *profile_number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rf-network** *name* **Example:** `Device (config)# wireless rf-network test1`	Creates an RF group. The group name should be ASCII String up to 19 characters and is case sensitive. **Note** Repeat this procedure for each controller that you want to include in the RF group.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 4	**show network profile** *profile_number*	Displays the RF group. **Note** You can view the network profile number from 1 to 4294967295.

Configuring Members in a 802.11 Static RF Group (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* **Example:** `Device(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	Configures members in a 802.11 static RF group. The group mode should be set as leader for the group member to be active.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Transmit Power Control

Configuring the Tx-Power Control Threshold (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm tpc-threshold -60`	Configures the Tx-power control threshold used by RRM for auto power assignment. The range is from –80 to –50.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Tx-Power Level (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm txpower** {*trans_power_level* | **auto** | **max** | **min** | **once**}

3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm txpower** {*trans_power_level* | **auto | max | min | once**} **Example:** `Device(config)#ap dot11 24ghz rrm txpower auto`	Configures the 802.11 tx-power level • **trans_power_level**—Sets the transmit power level. • **auto**—Enables auto-RF. • **max**—Configures the maximum auto-RF tx-power. • **min**—Configures the minimum auto-RF tx-power. • **once**—Enables one-time auto-RF.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**}
3. **ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {*channel number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
4. **ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80** | **best**}
5. **ap dot11** {**24ghz** | **5ghz**} **rrm channel device**
6. **ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign**
7. **ap dot11** {**24ghz** | **5ghz**} **rrm channel load**
8. **ap dot11** {**24ghz** | **5ghz**} **rrm channel noise**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} **Example:** `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures CleanAir event-driven RRM parameters. • **High**–Specifies the most sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value. • **Low**–Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value. • **Medium**–Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {*channel number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
	Example:
	`Device(config)#ap dot11 24ghz rrm channel dca interval 2`
		Configures Dynamic Channel Assignment (DCA) algorithm parameters for the 802.11 band.
		• ***<1-14>***–Enter a channel number to be added to the DCA list.
		• **anchor-time**–Configures the anchor time for the DCA. The range is between 0 and 23 hours.
		• **global**–Configures the DCA mode for all 802.11 Cisco APs.
		  • **auto**–Enables auto-RF.
		  • **once**–Enables auto-RF only once.
		• **interval**–Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes.
		• **min-metric**–Configures the DCA minimum RSSI energy metric. The range is between -100 and -60.
		• **sensitivity**–Configures the DCA sensitivity level to changes in the environment.
		  • **high**–Specifies the most sensitivity.
		  • **low**–Specifies the least sensitivity.
		  • **medium**–Specifies medium sensitivity.

Step 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80** | **best**}	Configures the DCA channel width for all 802.11 radios in the 5-GHz band. Sets the channel width to 20 MHz, 40 MHz, 80 MHz, or Best; 20 MHz is the default value.
Step 5	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** **Example:** `Device(config)#ap dot11 24ghz rrm channel device`	Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.

	Command or Action	Purpose
Step 6	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** **Example:** `Device(config)#ap dot11 24ghz rrm channel foreign`	Configures the foreign AP 802.11 interference avoidance in the channel assignment.
Step 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** **Example:** `Device(config)#ap dot11 24ghz rrm channel load`	Configures the Cisco AP 802.11 load avoidance in the channel assignment.
Step 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** **Example:** `Device(config)#ap dot11 24ghz rrm channel noise`	Configures the 802.11 noise avoidance in the channel assignment.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Coverage Hole Detection (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**}
3. **ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level*
4. **ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level*
5. **ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} **Example:** `Device(config)#ap dot11 24ghz rrm coverage data fail-percentage 60`	Configures the 802.11 coverage hole detection for data packets. • **fail-percentage**—Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.

	Command or Action	Purpose
		• **packet-count**—Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255. • **rssi-threshold**—Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.
Step 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level* **Example:** `Device(config)#ap dot11 24ghz rrm coverage exception global 50`	Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level* **Example:** `Device(config)#ap dot11 24ghz rrm coverage level global 10`	Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.
Step 5	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} **Example:** `Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10`	Configures the 802.11 coverage hole detection for voice packets. • **fail-percentage**—Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%. • **packet-count**—Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255. • **rssi-threshold**—Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Event Logging (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**}
	Example:
	`Device(config)#ap dot11 24ghz rrm logging channel`
	`Device(config)#ap dot11 24ghz rrm logging coverage`
	`Device(config)#ap dot11 24ghz rrm logging foreign`
	`Device(config)#ap dot11 24ghz rrm logging load`
	`Device(config)#ap dot11 24ghz rrm logging noise`
	`Device(config)#ap dot11 24ghz rrm logging performance`
	`Device(config)#ap dot11 24ghz rrm logging txpower`
		Configures event-logging for various parameters.
		• **channel**—Configures the 802.11 channel change logging mode.
		• **coverage**—Configures the 802.11 coverage profile logging mode.
		• **foreign**—Configures the 802.11 foreign interference profile logging mode.
		• **load**—Configures the 802.11 load profile logging mode.
		• **noise**—Configures the 802.11 noise profile logging mode.
		• **performance**—Configures the 802.11 performance profile logging mode.
		• **txpower**—Configures the 802.11 transmit power change logging mode.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Statistics Monitoring (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**}
3. **ap dot11 24ghz | 5ghz rrm monitor coverage** *interval*
4. **ap dot11 24ghz | 5ghz rrm monitor load** *interval*
5. **ap dot11 24ghz | 5ghz rrm monitor noise** *interval*
6. **ap dot11 24ghz | 5ghz rrm monitor signal** *interval*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} **Example:** `Device(config)#ap dot11 24ghz rrm monitor channel-list all`	Sets the 802.11 monitoring channel-list for parameters such as noise/interference/rogue. • **all**— Monitors all channels. • **country**— Monitor channels used in configured country code. • **dca**— Monitor channels used by dynamic channel assignment.
Step 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor coverage 600`	Configures the 802.11 coverage measurement interval in seconds that ranges from 60 to 3600.
Step 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor load 180`	Configures the 802.11 load measurement interval in seconds that ranges from 60 to 3600.
Step 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor noise 360`	Configures the 802.11 noise measurement interval (channel scan interval) in seconds that ranges from 60 to 3600.
Step 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor signal 480`	Configures the 802.11 signal measurement interval (neighbor packet frequency) in seconds that ranges from 60 to 3600.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11 Performance Profile (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value*
3. **ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value*
4. **ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value*
5. **ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value*
6. **ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile clients 20`	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.
Step 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile foreign 50`	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile noise -65`	Sets the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.
Step 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.

	Command or Action	Purpose
Step 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile utilization 75`	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before you begin

Ensure that each Cisco WLC 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 Cisco WLCs have different names, false alarms will occur.

SUMMARY STEPS

1. **ap name** *Cisco_AP* **mode** {**local** | **monitor**}
2. **end**
3. **configure terminal**
4. **wireless wps ap-authentication**
5. **wireless wps ap-authentication threshold** *value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode** {**local**	**monitor**} **Example:** `Device# ap name ap1 mode local`	Configures a particular access point for local (normal) mode or monitor (listen-only) mode. Perform this step for every access point connected to the Cisco WLC.
Step 2	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**wireless wps ap-authentication** **Example:** `Device (config)# wireless wps ap-authentication`	Enables rogue access point detection.
Step 5	**wireless wps ap-authentication threshold** *value* **Example:** `Device (config)# wireless wps ap-authentication threshold 50`	Specifies 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. 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. **Note** Enable rogue access point detection and threshold value on every Cisco WLC in the RF group. **Note** If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

Monitoring RRM Parameters and RF Group Status

Monitoring RRM Parameters

Table 1: Commands for monitoring Radio Resource Management

Commands	Description
show ap dot11 24ghz ccx	Displays the 802.11b CCX information for all Cisco APs.
show ap dot11 24ghz channel	Displays the configuration and statistics of the 802.11b channel assignment.
show ap dot11 24ghz coverage	Displays the configuration and statistics of the 802.11b coverage.
show ap dot11 24ghz group	Displays the configuration and statistics of the 802.11b grouping.
show ap dot11 24ghz l2roam	Displays 802.11b l2roam information.
show ap dot11 24ghz logging	Displays the configuration and statistics of the 802.11b event logging.
show ap dot11 24ghz monitor	Displays the configuration and statistics of the 802.11b monitoring.

Commands	Description
show ap dot11 24ghz profile	Displays 802.11b profiling information for all Cisco APs.
show ap dot11 24ghz receiver	Displays the configuration and statistics of the 802.11b receiver.
show ap dot11 24ghz summary	Displays the configuration and statistics of the 802.11b Cisco APs.
show ap dot11 24ghz txpower	Displays the configuration and statistics of the 802.11b transmit power control.
show ap dot11 5ghz ccx	Displays 802.11a CCX information for all Cisco APs.
show ap dot11 5ghz channel	Displays the configuration and statistics of the 802.11a channel assignment.
show ap dot11 5ghz coverage	Displays the configuration and statistics of the 802.11a coverage.
show ap dot11 5ghz group	Displays the configuration and statistics of the 802.11a grouping.
show ap dot11 5ghz l2roam	Displays 802.11a l2roam information.
show ap dot11 5ghz logging	Displays the configuration and statistics of the 802.11a event logging.
show ap dot11 5ghz monitor	Displays the configuration and statistics of the 802.11a monitoring.
show ap dot11 5ghz profile	Displays 802.11a profiling information for all Cisco APs.
show ap dot11 5ghz receiver	Displays the configuration and statistics of the 802.11a receiver.
show ap dot11 5ghz summary	Displays the configuration and statistics of the 802.11a Cisco APs.
show ap dot11 5ghz txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Monitoring RF Group Status (CLI)

This section describes the new commands for RF group status.

The following commands can be used to monitor RF group status on the .

Table 2: Monitoring Aggressive Load Balancing Command

Command	Purpose
show ap dot11 5ghz group	Displays the Cisco WLC name which is the RF group leader for the 802.11a RF network.
show ap dot11 24ghz group	Displays the Cisco WLC name which is the RF group leader for the 802.11b/g RF network.

Examples: RF Group Configuration

This example shows how to configure RF group name:

```
Device# configure terminal
Device(config)# wireless rf-network test1
Device(config)# ap dot11 24ghz shutdown
Device(config)# end
Device # show network profile 5
```

This example shows how to configure rogue access point detection in RF groups:

```
Device# ap name ap1 mode local
Device# end
Device# configure terminal
Device(config)# wireless wps ap-authentication
Device(config)# wireless wps ap-authentication threshold 50
Device(config)# end
```

Information About ED-RRM

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.

Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)

Step 1 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:

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** —Configures CleanAir driven RRM parameters for the 802.11 Cisco lightweight access points.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Configures CleanAir driven RRM sensitivity for the 802.11 Cisco lightweight access points. Default selection is Medium.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**—Enables rogue contribution.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contributionduty-cycle** *thresholdvalue*—Configures threshold value for rogue contribution. The valid range is from 1 to 99, with 80 as the default.

Step 2 Save your changes by entering this command:

write memory

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

show ap dot11 {24ghz | 5ghz} cleanair config

Information similar to the following appears:

```
AdditionalClean Air Settings:
CleanAir Event-driven RRM State.............. : Enabled
CleanAir Driven RRM Sensitivity.............. : LOW
CleanAir Event-driven RRM Rogue Option....... : Enabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state............ : Disabled
CleanAir Persistent Device Propagation....... : Disabled
```

Additional References for Radio Resource Management

Related Documents

Related Topic	Document Title
RRM commands and their details	*RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Radio Resource Management Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.