Radio Resource Management

Information About Radio Resource Management

The Radio Resource Management (RRM) software that is embedded in the device acts as a built-in Radio Frequency (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
- Power control transmission

- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping

Note RRM grouping does not occur when an AP operates in a static channel that is not in the DCA channel list. The Neighbor Discovery Protocol (NDP) is sent only on DCA channels; therefore, when a radio operates on a non-DCA channel, it does not receive NDP on the 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 the associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can scan all the valid channels for the country of operation as well as for channels available in other locations. The access points in local mode go *offchannel* for a period not greater than 70 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), access points can defer off-channel measurements. The access points also defer off-channel measurements based on the WLAN scan priority configurations.

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

Transmit Power Control

The device dynamically controls access point transmit power based on the 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.

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.

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. Devices 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 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 simultaneously use 11 or 54 Mbps. By effectively reassigning channels, the device 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 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 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 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 huge 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 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 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 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-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 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.

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.

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.

How to Configure RRM

Configuring Neighbor Discovery Type (CLI)

Procedure

	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 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 Transmit Power Control

Configuring the Tx-Power Control Threshold (CLI)

Procedure

	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)

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	

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.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

Procedure

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

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.

	Command or Action	Purpose

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** { | **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.
		• –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**} **Example:** `Device(config)#ap dot11 5ghz rrm channel dca chan-width best`	Configures the DCA channel bandwidth for all 802.11 radios in the 5-GHz band. Sets the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz, ; 20 MHz is the default value for channel bandwidth. 80 MHz is the default value for best. Set the channel bandwidth to best before configuring the constraints.
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)

Procedure

	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%.
		• **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.

	Command or Action	Purpose

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)

Procedure

	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 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)

Procedure

	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.

	Command or Action	Purpose
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)

Procedure

	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:**	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz rrm profile clients 20`	
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.
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.

Configuring Advanced 802.11 RRM

Enabling Channel Assignment (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel-update** **Example:** `Device# ap dot11 24ghz rrm channel-update`	Enables the 802.11 channel selection update for each of the Cisco access points. **Note** After you enable **ap dot11 {24ghz | 5ghz} rrm channel-update**, a token is assigned for channel assignment in the DCA algorithm.

Restarting DCA Operation

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm dca restart** **Example:** `Device# ap dot11 24ghz rrm dca restart`	Restarts the DCA cycle for 802.11 radio.

Updating Power Assignment Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm txpower update** **Example:** `Device# ap dot11 24ghz rrm txpower update`	Updates the 802.11 transmit power for each of the Cisco access points.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before you begin

Ensure that each embedded 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 embedded controller have different names, false alarms will occur.

Procedure

	Command or Action	Purpose
Step 1	**Example:** `Device#`	Perform this step for every access point connected to the embedded controller. • **monitor**:Sets the AP mode to monitor mode. • **clear**: Resets AP mode to local or remote based on the site. • **sensor**: Sets the AP mode to sensor mode. • **sniffer**: Sets the AP mode to wireless sniffer mode.

Step 2	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

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.

	Command or Action	Purpose
		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 embedded controller in the RF group. **Note** If rogue access point detection is not enabled on every embedded controller in the RF group, the access points on the embedded controller 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 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 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.
show ap dot11 24ghz profile	Displays 802.11b profiling information for all Cisco APs.
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 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 logging	Displays the configuration and statistics of the 802.11a event logging.

Commands	Description
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 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.

Verifying RF Group Status (CLI)

This section describes the new commands for RF group status.

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

Table 2: Verifying Aggressive Load Balancing Command

Command	Purpose
show ap dot11 5ghz group	Displays the controller name which is the RF group leader for the 802.11a RF network.
show ap dot11 24ghz group	Displays the controller 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#
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.

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

Procedure

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-contribution duty-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:

Information About Rogue PMF Containment

From Cisco IOS XE Dublin 17.12.1, the controller will contain a rogue AP with 802.11w Protected Management Frame (PMF) on centrally switched WLANs if the client-serving radio channel of a rogue-detecting AP matches the channel of the corresponding rogue AP.

PMF Containment is performed in the following scenarios:

- PMF containment is supported only in the local mode.
- PMF containment is done only for rogue clients that have not joined a rogue AP.
- PMF containment is done only if a rogue-detecting AP shares the same primary channel with a rogue client.

- PMF containment is not done on DFS channels even if a DFS channel is being used as a client-serving channel.
- PMF containment is effective only if there is at least one functioning WLAN on the serving radio where the containment is being performed.

The Rogue PMF Containment feature is supported only on the following APs:

- Cisco Catalyst 9130AX
- Cisco Catalyst 9136
- Cisco Catalyst 9162
- Cisco Catalyst 9164
- Cisco Catalyst 9166

Enabling Rogue PMF Containment

Follow this procedure to configure PMF containment on a per site basis.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**rogue detection containment pmf-denial** **Example:** `Device(config-ap-profile)# rogue detection containment pmf-denial`	Enables PMF-denial rogue AP containment.
Step 4	**pmf-deauth** **Example:** `Device(config-pmf-denial)# pmf-deauth`	Enables PMF-denial type deauthentication rogue AP containment.

Step 5	**end**
	Example:
	`Device(config-ap-profile)# end`
		Returns to privileged EXEC mode.

Verifying PMF Containment

To verify PMF containment and the relevant statistics, use the following commands.

To view the containment details summary for all the AP radios, use the following command:

```
Device# show wireless wps rogue containment summary

Rogue Containment activities for each managed AP

AP: 687d.b45f.2ae0  Slot: 1
  Active Containments    : 3
   Containment Mode      : DEAUTH_PMF
   Rogue AP MAC          : 687d.b45f.2a2d
   Containment Channels : 40
```

To verify the rogue statistics, use the following command:

```
Device# show wireless wps rogue stats
.
.
.
 States
  Alert                          : 256
  Internal                       : 0
  External                       : 0
  Contained                      : 1
  Containment-pending            : 0
  Threat                         : 0
  Pending                        : 0
Rogue Clients
  Total/Max Scale                : 20/16000
  Contained                      : 0
  Containment-pending            : 0
.
.
.
```

Information About Rogue Channel Width

From Cisco IOS XE Dublin 17.12.1, you can specify the channel width and the band for rogue detection. The newly introduced **condition chan-width** command allows you to set the minimum or maximum channel width for rogue detection. Only the rogue APs matching the channel width criteria and band are selected for rogue detection.

Configuring Rogue Channel Width (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue rule** *rule-name* **priority** *priority* **Example:** `Device(config)# wireless wps rogue rule 1 priority 1`	Creates or enables a rule.

Step 3	**condition chan-width** {**160MHz** | **20MHz** | **40MHz** | **80MHz**}**band**{**2.4GHz** | **5GHz** | **6GHz**}
	Example:
	`Device(config-rule)# condition chan-width 20MHz band 5gHz`
		Configures channel width and band for rogue detection.
		If the classification is **Friendly**, this is the minimum channel width.
		If the classification is **Custom**, **Malicious**, or **Delete**, this is the maximum channel width.

Step 4	**Use either Step 4** > **5** > **6** > **7**	**Note** Use only one of the Steps: 4, 5, 6 or 7 as required to classify rogue devices. Do not use all of them.

Step 5	**classify friendly state** {**alert** | **external** | **internal** }
	Example:
	`Device(config-rule)# classify friendly state internal`
		(Optional) Classifies devices matching this rule as friendly.
		• **alert**: Sets the malicious rogue access point to alert mode.
		• **external**: Acknowledges the presence of a rogue access point.
		• **internal**: Trusts a foreign access point.

Step 6	**classify malicious state** {**alert** | **contained** }
	Example:
	`Device(config-rule)# classify malicious state alert`
		(Optional) Classifies devices matching this rule as malicious.
		• **alert**: Sets the malicious rogue access point to alert mode.
		• **contained**: Contains the rogue access point.

Step 7	**classify custom severity-score** *severity-score* [**name** *name*] **state** {**alert** | **contained** }	(Optional) Classifies devices matching this rule as custom.

	Command or Action	Purpose
	Example: `Device(config-rule)# classify custom severity-score 12 name rule1 state alert`	• *severity-score* : Custom classification severity score. Valid values range from 1 to 100. • **name**: Defines the name for custom classification. • *name* : Custom classification name. • **state**: Defines the final state if rule is matched. • **alert**: Sets the rogue access point to alert mode. • **contained**: Contains the rogue access point.
Step 8	**classify delete** **Example:** `Device(config-rule)# classify delete`	Ignoores the devices matching this rule.

Step 9	**end**
	Example:
	`Device(config-rule)# end`
		Returns to privileged EXEC mode.

Configuring Rogue Classification Rules (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **Rogue AP Rules** to open the **Rogue Rules** window.

Rules that have already been created are listed in priority order. The name, type, status, state, match, and hit count of each rule is provided.

Note To delete a rule, select the rule and click **Delete**.

Step 2 Create a new rule as follows:

a) Click **Add**.
b) In the **Add Rogue AP Rule** window that is displayed, enter a name for the new rule, in the **Rule Name** field. Ensure that the name does not contain any spaces.
c) From the **Rule Type** drop-down list, choose one of the following options to classify rogue access points matching this rule:

- **Friendly**
- **Malicious**

- **Unclassified**
- **Custom**

d) Configure the state of the rogue AP from the **State** drop-down list. This is the state when the rule matches the conditions for the rogue APs.

- **Alert**: A trap is generated when an ad hoc rogue is detected.
- **Internal**: A foreign ad hoc rogue is trusted.
- **External**: The presence of an ad hoc rogue is acknowledged.
- **Contain**: The ad hoc rogue is contained.
- **Delete**: The ad hoc rogue is removed.

Note The **State** field is not displayed if you select **Unclassified** as the **Rule Type**.

e) If you chose the **Rule Type** as **Custom**, enter the **Severity Score** and the **Custom Name**.

f) Click **Apply to Device** to add this rule to the list of existing rules, or click **Cancel** to discard this new rule.

Step 3 (Optional) Edit a rule as follows:

a) Click the name of the rule that you want to edit.

b) In the **Edit Rogue AP Rule** page that is displayed, from the **Type** drop-down list, choose one of the following options to classify rogue access points matching this rule:

- **Friendly**
- **Malicious**
- **Custom**

c) Configure the notification from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None** after the rule is matched.

d) Configure the state of the rogue AP from the **State** drop-down list after the rule is matched.

e) From the **Match Operation** field, choose one of the following:

- **Match All**: The detected rogue access point must meet all of the conditions specified by the rule for the rule to be matched and the rogue access point to adopt the classification type of the rule.
- **Match Any**: The detected rogue access point must meet any of the conditions specified by the rule for the rule to be matched and the rogue access point to adopt the classification type of the rule. This is the default value.

f) To enable this rule, check the **Enable Rule** check box. The default is unchecked.

g) If you chose the **Rule Type** as **Custom**, enter the **Severity Score** and the **Classification Name**.

h) From the **Add Condition** drop-down list, choose one or more of the following conditions that the rogue access point must meet :

- **None**: No condition is set for rogue access point detection.
- **client-count**: Condition requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point can be classified as malicious. If you choose this

option, enter the minimum number of clients to be associated with the rogue access point in the **Minimum Number of Rogue Clients** field. The valid range is 1 to 10 (inclusive), and the default value is 0.

- **duration**: Condition requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the **Time Duration** field. The valid range is 0 to 86400 seconds (inclusive), and the default value is 0 seconds.
- **encryption**: Condition requires that the advertised WLAN have specified encryption. Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate with it. No further configuration is required for this option.
- **infrastructure**: Condition requires that the rogue access point's SSID (the SSID configured for the WLAN) be known to the controller. Select the **Manage SSID** check box to enable this configuration.
- **rssi**: Condition requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the **Maximum RSSI** field. The valid range is 0 to –128 dBm (inclusive).
- **channel-width**: Condition requires that the rogue access point use the specified radio spectrum channel width for the specified radio band, as defined below. The valid channel widths are 20, 40, 80, and 160MHz.
    - For APs to be classified as **Malicious**, **Custom** or **Delete**, it must match the value (equal or more) set in the **Minimum Channel Width** drop-down list.
    - For APs to be classified as **Friendly**, it must match the value (equal or less) set using an option from the **Maximum Channel Width** drop-down list.
- **ssid**: Condition requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the **User Configured SSID** text field, and click **+** to add the SSID.
- **substring-ssid**: Condition requires that the rogue access point have a substring of the specific user-configured SSID. The controller searches the substring in the same occurrence pattern and returns a match if the substring is found in the SSID string.

Step 4 Click **Apply to Device** to save the configuration.

Step 5 Click **OK**.

Verifying Rogue Channel Width

To view channel width and band information of a classification rule, use the following commands.

Note When the same BSSID is beaconing on multiple bands (2.4 GHz, 5 GHz, 6 GHz), the **show wireless wps rogue ap summary** command output displays information for the band with the highest RSSI.

```
Device# show wireless wps rogue rule detailed 1

Priority                                           : 1
Rule Name                                          : 1
Status                                             : Enabled
Type                                               : Friendly
State                                              : Alert
Match Operation                                    : Any
Notification                                       : Enabled
Hit Count                                          : 117
Condition :
  type                                             : chan-width
  Max value (MHz)                                  : 40
  Band (GHz)                                       : 5GHz

Device# wireless wps rogue ap summary
.
.
.

MAC Address     Classification  State  #APs  #Clients  Last Heard
Highest-RSSI-Det-AP  RSSI  Channel  Ch.Width  GHz
------------------------------------------------------------------------------------------
002c.c849.9f00  Unclassified    Alert  2     0         10/18/2022 16:50:18  0cd0.f895.efc0
       -31        11        20  2.4
0062.ecf3.e73f  Unclassified    Alert  1     0         10/18/2022 16:50:16  0cd0.f895.efc0
       -46        36        80  5
4ca6.4d22.cbaf  Unclassified    Alert  3     0         10/18/2022 16:50:46  0cd0.f895.efc0
       -62        36       160  5
```