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.

Information About RF Groups

An RF group is a logical collection of controllers that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. Separate RF groups exist for 2.4-GHz and 5-GHz networks. Clustering Cisco Catalyst 9800 Series Wireless Controller into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single Cisco Catalyst 9800 Series Wireless Controller.

An RF group is created based on the following parameters:

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

RF grouping runs between controllers .

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

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

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

RF Group Leader

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

Note RF Group Leader is selected based on the controller with the greatest AP capacity (platform limit). If multiple controllers have the same capacity, the leader is selected based on the Group ID, which is a combination of the management IP address, AP capacity, random number, and so on. The one with the highest Group ID is selected as the leader.

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

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

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

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

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

If Dynamic Channel Assignment (DCA) needs to use the worst-performing radio as the single criterion for adopting a new channel plan, it can result in pinning or cascading problems.

The main cause of both pinning and cascading is that any potential channel plan changes are controlled by the RF circumstances of the worst-performing radio. The DCA algorithm does not do this; instead, it does the following:

- Multiple local searches: The DCA search algorithm performs multiple local searches initiated by different radios in the same DCA run rather than performing a single global search that is 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 in an 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 the 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 Grouping Failure Reason Codes

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

Table 1: RF Grouping Failure Reason Codes

Reason Code	Description
1	Maximum number (20) of controllers are already present in the group.

Reason Code	Description
2	If the following conditions are met: • The request is from a similar powered controller and, • Controller is the leader for the other band, OR • Requestor group is larger.
3	Group ID do not match.
4	Request does not include source type.
5	Group spilt message to all member while group is being reformed.
6	Auto leader is joining a static leader, during the process deletes all the members.
9	Grouping mode is turned off.
11	Country code does not match.
12	Controller is up in hierarchy compared to sender of join command (static mode). Requestor is up in hierarchy (auto mode).
13	Controller is configured as static leader and receives join request from another static leader.
14	Controller is already a member of static group and receives a join request from another static leader.
15	Controller is a static leader and receives join request from non-static member.
16	Join request is not intended to the controller. Controller name and IP do not match.
18	RF domain do not match.
19	Controller received a Hello packet at incorrect state.
20	Controller has already joined Auto leader, now gets a join request from static leader.
21	Group mode change. Domain name change from CLI. Static member is removed from CLI.
22	Max switch size (350) is reached

Additional Reference

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

RF Group Name

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

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

Rogue Access Point Detection in RF Groups

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

Secure RF Groups

Secure RF groups enable to encrypt and secure RF grouping and RRM message exchanges over DTLS tunnel. During the DTLS handshake controllers authenticate each other with wireless management trust-point certificate.

Note If a controller has to be part of secure RF-group, that controller must be part of the same mobility group.

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.

Cisco APs support power level changes in 3 dB granularity. TPC Min and Max power settings allow for values in 1 dB increments. The resulting power level will be rounded to the nearest value supported in the allowed powers entry for the AP model and the current serving channel.

Each AP model has its own set of power levels localized for its regulatory country and region. Moreover, the power levels for the same AP model will vary based on the band and channel it is set to. For more information on Allowed Power Level vs. Actual power(in dBm), use the **show ap name <name> config slot <0|1|2|3>** command to view the specific number of power levels, the range of power levels allowed, and the current power level setting on the AP.

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 DCA supports only 20-MHz channels in 2.4-GHz band.

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.

Invoking channel update will not result in any immediate changes until the next DCA interval is triggered.

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.

Dynamic Bandwidth Selection

While upgrading from 11n to 11ac, the Dynamic Bandwidth Selection (DBS) algorithm provides a smooth transition for various configurations.

The following pointers describe the functionalities of DBS:

- It applies an additional layer of bias on top of those applied to the core DCA, for channel assignment in order to maximize the network throughput by dynamically varying the channel width.
- It fine tunes the channel allocations by constantly monitoring the channel and Base Station Subsystem (BSS) statistics.
- It evaluates the transient parameters, such as 11n or 11ac client mix, load, and traffic flow types.
- It reacts to the fast-changing statistics by varying the BSS channel width or adapting to the unique and new channel orientations through 11ac for selection between 40 MHz and 80 MHz bandwidths.

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.

Cisco AI Enhanced RRM

The AI Enhanced RRM is the next evolution of Cisco's award winning Radio Resource Management (RRM).

The RRM runs as a service in a Cisco Catalyst 9800 Series Wireless Controller. The Cisco RRM manages the RF Group (the components making up the RF Network) based on dynamic measurements between every AP and its neighbors stored in a local database for the entire RF Group. At runtime, the RRM draws the last 10 minutes of the collected data, and gently optimizes based on the current network conditions.

The AI Enhanced RRM integrates the power of Artificial Intelligence and Machine Learning to the reliable and trusted Cisco RRM product family algorithms in the Cloud.

Note The AI enhanced RRM is coordinated through the Cisco Catalyst Center (on-prem appliance) as a service. The current RRM sites are seamlessly transitioned to an intelligent centralized service. AI enhanced RRM along with other Cisco Catalyst Center services brings a host of new features with it.

Cisco AI Enhanced RRM operates as a distributed RRM service. RF telemetry is collected from the Cisco Access Points by the controller, and passed through the Catalyst Center to the Cisco AI Analytics Cloud where the data is stored. The RRM Algorithms run against this telemetry data stored in the cloud. AI analyzes the solutions, and passes any configuration change information back to the Catalyst Center. The Catalyst Center maintains the control connection with the enrolled controller and passes any individual AP configuration changes back to the APs.

The following RRM algorithms run in the cloud while the remaining work in the controller:

- DCA
- TPC
- DBS
- FRA

Note The RRM algorithms run in the cloud against the telemetry data available in the cloud.

If the location of controller, and APs are provisioned previously, assigning a location enrolls the AI Enhanced RRM Services and the profile to be pushed to the controller. Thus, AI Enhanced RRM becomes the RF Group Leader for the subscribed controller.

For more information on the Cisco Catalyst Center, see Cisco Catalyst Center User Guide.

Note The following table covers the controller and Cisco Catalyst Center release versions that support Cisco AI Enhanced RRM support:

Table 2: Controller and Cisco Catalyst Center Releases Supporting Cisco AI Enhanced RRM Support

Controller Release	Cisco Catalyst Center Release	Cisco AI Enhanced RRM Support
Cisco IOS XE Cupertino 17.9.x	• Cisco Catalyst Center, Release 2.3.2 or Cisco Catalyst Center, Release 2.3.3 • Cisco Catalyst Center, Release 2.3.4	• 2.4GHz and 5GHz • 2.4GHz, 5GHz, and 6GHz
Cisco IOS XE Cupertino 17.8.x	• Cisco Catalyst Center, Release 2.3.2 Cisco Catalyst Center, Release 2.3.3 • Cisco Catalyst Center, Release 2.3.4	2.4GHz and 5GHz
Cisco IOS XE Cupertino 17.7.x	Cisco Catalyst Center, Release 2.3.2 or Cisco Catalyst Center, Release 2.3.3	2.4GHz and 5GHz

Restrictions for Radio Resource Management

- The number of APs in a RF-group is limited to 3000.
- 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.
- Disabling all data rates for default rf-profile or custom rf-profile, impacts ISSU upgrade and client join process after the software upgrade (ISSU or non-ISSU). To prevent this, you must enable at least one data rate (for example, **ap dot11 24 rate RATE_5_5M enable**) on the default rf-profile or custom rf-profile. We recommend that you enable the lowest data rate if efficiency is of prime concern.
- Keywords such as secure cannot be used a RF group name.

How to Configure RRM

Configuring Neighbor Discovery Type (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **Radio Resource Management** page, click either the **5 GHz Band**, **2.4 GHz Band** or the **6 GHz Band** tab.

Step 3 In the **General** tab, under each section enter the corresponding field details:

a) Under the **Profile Threshold For Traps** section, enter the:

1. **Interference Percentage**: The foreign interference threshold is between 0 and 100 %. The default is 10 %.
2. **Clients**: The client threshold between 1 and 75 clients. The default is 12.
3. **Noise**: The foreign noise threshold between –127 dBm and 0dBm. The default is –70 dBm.
4. **Utilization Percentage**: The RF utilization threshold between 0 and 100 %. The default is 80 %.
5. **Throughput**: The average rate of successful messages delivery over a communication channel. Value ranges from 1000 to 1000000 bps.

b) Under the **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels** section, choose the:

1. **Channel List** from the drop-down list:
   - All Channels
   - Country Channels
   - DCA Channels
2. **RRM Neighbor Discover Type** from the drop-down list:
   - **Transparent**: Packets are sent as is.
   - **Protected**: Packets are protected.
3. **RRM Neighbor Discovery Mode**:
   - **AUTO**: If the NDP mode configured is AUTO, the controller selects On-Channel as the NDP mode. The default is set as AUTO.
   - **OFF-CHANNEL**: If the NDP mode configured is Off-Channel, the controller selects Off-Channel as the NDP mode.

c) Under the **Monitor** section, set:

- **Neighbor Packet Frequency (seconds)**: Frequency (in seconds) in which the Neighbor Discovery Packets are sent. The default is 180 seconds.
- **Reporting Interval (seconds)**: The default is 180 seconds. Each channel dwell has to be completed within 180 seconds.
- **Neighbor Timeout factor**: Value in seconds used to determine when to prune access points from the neighbor list that have timed out. The default is 20 seconds.

Step 4 Click Apply to save your configuration.

Configuring Neighbor Discovery Type (CLI)

Procedure

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

Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **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 When the multiple-country feature is being used, all controllers intended to join the same RF group must be configured with the same set of countries, configured in the same order.

Configuring RF Group Selection Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **RRM** page, click the relevant band's tab: either **6 GHz Band**, **5 GHz Band**, or **2.4 GHz Band**.

Step 3 Click the **RF Grouping** tab.

Step 4 Choose the appropriate **Group Mode** from these options:

- Automatic: 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

Note When AI Enhanced RRM is enabled on a controller and Cisco Catalyst Center is connected to a wireless network, Cisco Catalyst Center is assigned the group role as a leader. Controllers, managed by Cisco Catalyst Center and enabled with AI Enhanced RRM, are assigned the group role as remote members irrespective of the group mode they were previously assigned. The **Group Role** field will display as **Remote Member** and the **Group leader** field will display the IP address of the Cisco Catalyst Center.

Step 5 Save the configuration.

Configuring RF Group Selection Mode (CLI)

Procedure

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

Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} 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)

Procedure

	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.

Configuring a Secure RF Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rf-network secure** **Example:** `Device(config)# wireless rf-network secure`	Creates a secure RF group.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Step 4	**show ap dot11 {24ghz | 5ghz | 6ghz} group** **Example:** `Device# show ap dot11 24ghz group`	Displays configuration and statistics of 6-GHz band grouping.

Configuring Members in an 802.11 Static RF Group (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **RRM** page, click either the **6 GHz Band**, **5 GHz Band** or **2.4 GHz Band** tab.

Step 3 Click the **RF Grouping** tab.

Step 4 Choose the appropriate **Group Mode** from the following options:

- **Automatic(default)**: Members of an RF group elect an RF group leader to maintain a primary power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).
- **Leader**: A device 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 members' management IP addresses and system name are used to request the member to join the leader. The leader tries to establish a connection with a member every 1 minute if the member has not joined in the previous attempt.
- **Off**: No RF group is configured.

Step 5 Under **Group Members** section, click **Add**.

Step 6 In the **Add Static Member** window that is displayed, enter the controller name and the IPv4 or IPv6 address of the controller.

Step 7 Click **Save & Apply to Device**.

Configuring Members in an 802.11 Static RF Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} 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 Transmit Power (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **6 GHz Band**, **5 GHz Band**, or **2.4 GHz Band** tab, click the **TPC** tab.

Step 3 Choose of the following dynamic transmit power assignment modes:

- *Automatic*(default): The transmit power is periodically updated for all APs that permit this operation.
- *On Demand*: The transmit power is updated on demand. If you choose this option, you get to view the **Invoke Power Update Once**. Click **Invoke Power Update Once** to apply the RRM data successfully.
- *Fixed*: No dynamic transmit power assignments occur and values are set to their global default.

Step 4 Enter the maximum and minimum power level assignment on this radio. If you configure 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. The range is –10 dBm to 30 dBm.

Step 5 In the **Power Threshold** field, enter the cutoff signal level used by RRM when determining whether to reduce an access point’s power.

The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value can be changed when access points are transmitting at higher (or lower) than desired power levels. The range for this parameter is –80 to –50 dBm.

Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect. In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

Step 6 Click **Apply**.

Configuring the Tx-Power Control Threshold (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 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:** `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	**ap dot11 6ghz rrm txpower** *trans_power_level* **auto** **Example:** `Device(config)#ap dot11 6ghz rrm txpower auto`	Configures the 802.11 6-GHz tx-power level. • *trans_power_level*: Sets the transmit power level. Valid values range from 1 to 5. • **auto**: Enables auto-RF.

	Command or Action	Purpose
		Note The 6-GHz band uses constant-PSD instead of constant-EIRP, which allows the transmission at higher power as channel width increases. The power levels are derived based on the configured channel width. At the higher power levels between 1-3, these power values exceed the limit for legacy rate frames, like beacons. As a result, there is no change in the beacon power for higher levels, unlike the 2.4-GHz and 5-GHz bands.

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **DCA** tab, choose a **Channel Assignment Mode** to specify the DCA mode:

- *Automatic*(default)—Causes the device to periodically evaluate and, if necessary, update the channel assignment for all joined APs.
- *Freeze*—Causes the device to evaluate and update the channel assignment for all joined APs. If you choose this option, you get to view the Invoke Channel Update Once. Click **Invoke Channel Update Once** to apply the RRM data successfully.
- *Off*—Turns off DCA and sets all AP radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.

Step 3 From the **Interval** drop-down list, choose the interval that tells how often the DCA algorithm is allowed to run. The default interval is 10 minutes.

Step 4 From the **AnchorTime** drop-down list, choose a number to specify the time of day when the DCA algorithm must start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 5 Check the **Avoid Foreign AP Interference** check box to cause the device's RRM algorithms to consider 802.11 traffic from foreign APs (those not included in your wireless network) when assigning channels to lightweight APs, or uncheck it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign APs. By default, this feature is in enabled state.

Step 6 Check the **Avoid Cisco AP Load** check box to cause the device's RRM algorithms to consider 802.11 traffic from Cisco lightweight APs in your wireless network when assigning channels. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. By default, this feature is in disabled state.

Step 7 Check the **Avoid Non-802.11a Noise** check box to cause the device's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight APs. For example, RRM may have APs avoid channels with significant interference from non-AP sources, such as microwave ovens. By default, this feature is in enabled state.

Step 8 Check the **Avoid Persistent Non-Wi-Fi Interference** check box to enable the device to take into account persistent non-Wi-Fi interference in DCA calculations. A persistent interfering device is any device from the following categories, which has been seen in the past 7 days - Microwave Oven, Video Camera, Canopy, WiMax Mobile, WiMax Fixed, Exalt Bridge. With **Avoid Persistent Non-Wi-Fi Interference** enabled, if a Microwave Oven is detected, that interference from the Microwave Oven is taken into account in the DCA calculations for the next 7 days. After 7 days, if the interfering device is not detected anymore, it is no longer considered in the DCA calculations.

Step 9 From the **DCA Channel Sensitivity** drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- *Low*—The DCA algorithm is not particularly sensitive to environmental changes. The DCA threshold is 30 dB.
- *Medium* (default)—The DCA algorithm is moderately sensitive to environmental changes. The DCA threshold is 15 dB.
- *High* —The DCA algorithm is highly sensitive to environmental changes. The DCA threshold is 5 dB.

Step 10 Set the **Channel Width** as required. You can choose the RF channel width as 20 MHz, 40 MHz, 80 MHz, 160 MHz, or Best. This is applicable only for 802.11a/n/ac (5 GHZ) radio.

Step 11 The **Auto-RF Channel List** section shows the channels that are currently selected. To choose a channel, check the corresponding check box.

Note If you disable the serving radio channel of the root AP from the **Auto-RF Channel List**, you will not be able to view the neighboring APs in the root APs.

Step 12 In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference. If enabled, set the sensitivity threshold level at which the RRM is invoked, enter the custom threshold, and check the **Rogue Contribution** check box to enter the rogue duty-cycle.

Step 13 Click **Apply**.

Configuring Advanced 802.11 Channel Assignment Parameters (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 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 6ghz rrm channel dca** {**anchor-time** *0-23* | **global auto** | **interval** *0-24* | **sensitivity** {**high** | **low** | **medium**}}
	Example:
	`Device(config)#ap dot11 6ghz rrm channel`
	`dca interval 2`
		Configures 802.11 6GHz dynamic channel assignment algorithm parameters.
		• **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.
		• **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.
		• **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**}
	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.

	Command or Action	Purpose

Step 5	**ap dot11 5ghz rrm channel dca chan-width width-max** {**WIDTH_20MHz** | **WIDTH_40MHz** | **WIDTH_80MHz** | **WIDTH_MAX**}
	Example:
	`Device(config)#`**`ap dot11 5ghz rrm channel`**
	`dca chan-width width-max WIDTH_80MHz`
		Configures the maximum channel bandwidth that can be assigned to a channel. In this example, *WIDTH_80MHz* assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.

Step 6	**ap dot11 6ghz rrm channel dca chan-width width-max** {**WIDTH_20MHz** | **WIDTH_40MHz** | **WIDTH_80MHz** | **WIDTH_MAX**}
	Example:
	`Device(config)#`**`ap dot11 6ghz rrm channel`**
	`dca chan-width width-max WIDTH_80MHz`
		Configures the maximum channel bandwidth that can be assigned to a channel. In this example, *WIDTH_80MHz* assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.

Step 7	**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.

Step 8	**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 9	**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 10	**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 11	**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 (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** to configure Radio Resource Management parameters for 802.11ax (6-GHz), 802.11a/n/ac (5-GHz) and 802.11b/g/n (2.4-GHz) radios.

Step 2 On the **Radio Resource Management** page, click **Coverage** tab.

Step 3 To enable coverage hole detection, check the **Enable Coverage Hole Detection** check box.

Step 4 In the **Data Packet Count** field, enter the number of data packets.

Step 5 In the **Data Packet Percentage** field, enter the percentage of data packets.

Step 6 In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 7 In the **Voice Packet Count** field, enter the number of voice data packets.

Step 8 In the **Voice Packet Percentage** field, enter the percentage of voice data packets.

Step 9 In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 10 In the **Minimum Failed Client per AP** field, enter the minimum number of clients on an AP with a signal-to-noise ratio (SNR) below the coverage threshold. Value ranges from 1 to 75 and the default value is 3.

Step 11 In the **Percent Coverage Exception Level per AP** field, enter the maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold and click **Apply**. Value ranges from 0 to 100% and the default value is 25%.

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 | 6ghz} 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.

	Command or Action	Purpose
		• **rssi-threshold**: Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.

Step 3	**ap dot11 6ghz rrm coverage data**{**fail-percentage** *fail-percentage-value* | **packet-count** *packet-count-value*}
	Example:
	`Device(config)#ap dot11 6ghz rrm coverage`
	`data fail-percentage 60`
		Configures the 802.11 6-GHz coverage hole detection for data packets.
		• **fail-percentage**: Configures the 802.11 6-GHz coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.

Step 4	**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 5	**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 6	**ap dot11 {24ghz | 5ghz | 6ghz} 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.

	Command or Action	Purpose
Step 7	**ap dot11 6ghz rrm coverage voice**{**fail-percentage** *fail-percentage-value* | **packet-count** *packet-count-value*} **Example:** `Device(config)#ap dot11 6ghz rrm coverage voice packet-count 10`	Configures the 802.11 6-GHz coverage hole detection for voice packets. • **fail-percentage**: Configures the 802.11 6-GHz coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%. • **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.

Step 8	**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.

Step 2	**ap dot11 24ghz | 5ghz | 6ghz 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`
		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.

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz rrm logging txpower`	

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 (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** to configure Radio Resource Management parameters for 802.11ax (6-GHz), 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios.

Step 2 In the **Monitor Intervals(60 to 3600secs)** section, proceed as follows:

a) To configure the 802.11 noise measurement interval (channel scan interval), set the **AP Noise Interval**. The valid range is from 60 to 3600 seconds.

b) To configure the 802.11 signal measurement interval (neighbor packet frequency), set the **AP Signal Strength Interval**. The valid range is from 60 to 3600 seconds.

c) To configure the 802.11 coverage measurement interval, set the **AP Coverage Interval**. The valid range is from 60 to 3600 seconds.

d) To configure the 802.11 load measurement, set the **AP Load Interval**. The valid range is from 60 to 3600 seconds.

Step 3 Click **Apply**.

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 | 6ghz} 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 | 6ghz} 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 | 6ghz} 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 | 6ghz} rrm monitor measurement** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor measurement 360`	Configures the 802.11 measurement interval in seconds that ranges from 60 to 3600.
Step 6	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor neighbor-timeout-factor** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor neighbor-timeout-factor 50`	Configures the 802.11 neighbor timeout-factor in seconds that ranges from 5 to 60.
Step 7	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor reporting** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor reporting 480`	Configures the 802.11 reporting interval in seconds that ranges from 60 to 3600.
Step 8	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor rssi-normalization** **Example:** `Device(config)#ap dot11 24ghz rrm monitor rssi-normalization`	Configures the 802.11 RRM Neighbor Discovery RSSI normalization.

Configuring the 802.11 Performance Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join** page, click the name of the profile or click **Add** to create a new one.

Step 3 In the **Add/Edit RF Profile** window, click the **RRM** tab.

Step 4 In the **General** tab that is displayed, enter the following parameters:

a) In the **Interference (%)** field, enter the threshold value for 802.11 foreign interference that ranges between 0 and 100 percent.

b) In the **Clients** field, enter the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.

c) In the **Noise (dBm)** field, enter the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.

d) In the **Utilization(%)** field, enter the threshold value for 802.11 RF utilization that ranges between 0 to 100 percent.

Step 5 Click **Update & Apply to Device**.

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:** `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 6ghz rrm profile customize** **Example:**	Enables performance profiles.

	Command or Action	Purpose
	`Device(config)#ap dot11 6ghz rrm profile customize`	
Step 6	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **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 7	**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 8	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring Advanced 802.11 RRM

Enabling Channel Assignment (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **RRM** page, click the relevant band's tab: either **6 GHz Band**, **5 GHz Band** or **2.4 GHz Band**.

Step 3 Click the **DCA** tab

Step 4 In the **Dynamic Channel Assignment Algorithm** section, choose the appropriate **Channel Assignment Mode** from these options:

- Automatic: Sets the channel assignment to automatic.
- Freeze: Locks the channel assignment. Click **Invoke Channel Update Once** to refresh the assigned channels.

Step 5 Click **Apply**.

Enabling Channel Assignment (CLI)

Procedure

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

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the AP name from the 5GHz or 2.4 GHz list.

Step 3 In the **Edit Radios** > **Configure** > **Tx Power Level Assignment** section, choose **Custom** from the **Assignment Method** group-down list.

Step 4 Choose the value for **Transmit Power** from the drop-down list.

Step 5 Click **Update & Apply to Device**.

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** | **6ghz**} **rrm txpower update** **Example:** `Device# ap dot11 24ghz rrm txpower update`	Initiates the update of the 802.11 6-Ghz transmit power for every Cisco AP.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before you begin

Ensure that each controller in the RF group has been configured with the same RF group name.

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

Procedure

	Command or Action	Purpose

Step 1	**ap name** *Cisco_AP* **mode**{**monitor** | **clear** | **sensor** | **sniffer**}
	Example:
	`Device# ap name ap1 mode clear`
		Perform this step for every access point connected to the controller .
		Configures the following AP modes of operation:
		• **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.

	Command or Action	Purpose

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

Monitoring RRM Parameters and RF Group Status

Monitoring RRM Parameters

Table 3: 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.

Commands	Description
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.
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 4: 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.
show ap dot11 6ghz group	Displays the controller name which is the RF group leader for the 802.11 6-GHz RF network.

To display the controller as a remote member and part of the AI Enhanced RRM, use the following command:

```
Device# show ap dot11 24ghz group
```

```
Radio RF Grouping

RF Group Name : Open-RRM
RF Protocol Version(MIN) : 100(30)
RF Packet Header Version : 2
802.11b Group Mode : AUTO
802.11b Group Role : Remote-Member
802.11b Group Update Interval : 600 seconds
802.11b Group Leader : 172.19.30.39 (172.19.30.39)
Secure-RRM : Disabled


RF Group Members

Controller name Controller IP Controller IPv6 DTLS status
-------------------------------------------------------------------------------------------
evwlc-188         192.1.0.188     N/A
```

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 clear
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. Once a channel change occurs due to event-driven RRM, the channel is blocked list for three hours to avoid selection. 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 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 custom-threshold** *custom-threshold-value*—Triggers the ED-RRM event at the set threshold value. The custom threshold values range from 1 to 99.

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:

```
CleanAir Solution................................ : Enabled
Air Quality Settings:
Air Quality Reporting........................ : Enabled
Air Quality Reporting Period (min)........... : 15
Air Quality Alarms........................... : Disabled
Air Quality Alarm Threshold.................. : 10
Unclassified Interference.................... : Disabled
Unclassified Severity Threshold.............. : 35
Interference Device Settings:
Interference Device Reporting................ : Enabled
BLE Beacon............................... : Enabled
Bluetooth Link........................... : Enabled
Microwave Oven........................... : Enabled
802.11 FH................................ : Enabled
Bluetooth Discovery...................... : Enabled
TDD Transmitter.......................... : Enabled
Jammer................................... : Enabled
Continuous Transmitter................... : Enabled
DECT-like Phone.......................... : Enabled
Video Camera............................. : Enabled
802.15.4................................. : Enabled
WiFi Inverted............................ : Enabled
WiFi Invalid Channel..................... : Enabled
SuperAG.................................. : Enabled
Canopy................................... : Enabled
Microsoft Device......................... : Enabled
```

```
WiMax Mobile............................. : Enabled
WiMax Fixed.............................. : Enabled
Interference Device Types Triggering Alarms:
BLE Beacon............................... : Disabled
Bluetooth Link........................... : Disabled
Microwave Oven........................... : Disabled
802.11 FH................................ : Disabled
Bluetooth Discovery...................... : Disabled
TDD Transmitter.......................... : Disabled
Jammer................................... : Disabled
Continuous Transmitter................... : Disabled
DECT-like Phone.......................... : Disabled
Video Camera............................. : Disabled
802.15.4................................. : Disabled
WiFi Inverted............................ : Enabled
WiFi Invalid Channel..................... : Enabled
SuperAG.................................. : Disabled
Canopy................................... : Disabled
Microsoft Device......................... : Disabled
WiMax Mobile............................. : Disabled
WiMax Fixed.............................. : Disabled
Interference Device Alarms................... : Disabled
AdditionalClean Air Settings:
CleanAir Event-driven RRM State.............. : Disabled
CleanAir Driven RRM Sensitivity.............. : LOW
CleanAir Driven RRM Sensitivity Level........ : 35
CleanAir Event-driven RRM Rogue Option....... : Disabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state............ : Disabled
CleanAir Persistent Device Propagation....... : Disabled
```

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**}	Configures channel width and band for rogue detection.

	Command or Action	Purpose
	Example: `Device(config-rule)# condition chan-width 20MHz band 5gHz`	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** }
	Example:
	`Device(config-rule)# classify custom severity-score 12 name rule1 state alert`
		(Optional) Classifies devices matching this rule as custom.
		• *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:**	Ignoores the devices matching this rule.

	Command or Action	Purpose
	`Device(config-rule)# classify delete`	

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
```