Radio Resource Management

- Radio resource management, on page 1
- How to configure RRM, on page 13
- Monitor RRM parameters and RF group status, on page 35
- Event-Driven Radio Resource Management , on page 36
- Rogue detection - rogue channel width, on page 39
- Rogue detection - rogue channel width, on page 44

Radio resource management

A Radio Resource Management (RRM) is a system that

- consistently manages real-time RF parameters of a wireless network
- monitors associated APs for traffic load, interference, noise, coverage, and other metrics,
- performs critical functions like radio resource monitoring, power control transmission, dynamic channel assignment, and coverage hole detection and correction.

Feature history

Table 1: Feature history table for radio resource management

Feature name	Release information	Feature description
Radio resource management	Cisco IOS XE 16.10.1	Radio Resource Management (RRM) is a feature that automates and optimizes the management of radio frequencies in a wireless network. It enables continuous monitoring of access points (APs) for metrics such as traffic load, interference, noise, and coverage.

Functions of radio resource management

- Radio Resource Monitoring: Ensures optimal allocation of network resources.

- Power Control Transmission: Adjusts power levels to maintain network performance.
- Dynamic Channel Assignment: Allocates channels dynamically to reduce interference and optimize network performance.
- Coverage Hole Detection and Correction: Identifies and rectifies gaps in coverage to ensure consistent connectivity.
- RF Grouping: Groups RF resources effectively to manage interference and optimize performance.

Radio resource monitors

Radio resource monitor is a system that

- detects and configures new devices and APs automatically
- adjusts associated APs for optimal coverage and capacity, and
- supports noise and interference monitoring.
- APs scan all the valid channels for the country of operation as well as for channels available in other locations.
- The APs 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 APs, rogue clients, ad-hoc clients, and interfering APs.
- In the presence of voice traffic or other critical traffic (in the last 100 ms), APs can defer off-channel measurements. The APs also defer off-channel measurements based on the WLAN scan priority configurations.
- Each AP spends only 0.2 percent of its time off channel. This activity is distributed across all the APs so that adjacent APs are not scanning at the same time, which could adversely affect wireless LAN performance.

Mobility controller and mobility agent

Radio frequency groups

A radio frequency group is a collection of controllers that

- coordinate RRM globally
- support separate networks for 2.4 GHz and 5 GHz networks, and
- optimize network calculations on a per-radio basis.

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.

RF group creation

Create an RF group using these parameters:

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

RF grouping function run between controllers .

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 neighborhood

APs periodically send out neighbor messages over the air. APs using the same RF group name validate messages from each other.

When APs 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.

RF group leader

An RF group leader is a designated device that

- analyzes real-time radio data collected by the system
- calculates power and channel assignments, and
- sends them to each controller in the RF group.

The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

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.

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

- Auto Mode: In this mode, the members of an RF group elect an RF group leader to maintain a *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.

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.

Pinning and cascading

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 2: RF Grouping Failure Reason Codes

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

Reason Code	Description
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

An RF group name is a user-configured identifier assigned to a group of wireless LAN controllers that

- is sent to all the access points joined to the controller
- coordinate to perform Radio Resource Management (RRM) in a globally optimized manner,
- serves as a shared secret for generating hashed MIC in neighbor messages, and
- helps in avoiding RF interference and contention by ensuring system-wide RRM.

To create an RF group, you configure all the controllers to be included in the group with the same RF group name. If there is any possibility that an AP joined to a controller might hear RF transmissions from an AP on a different controller , you should configure the controller with the same RF group name.

If RF transmissions between APs can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

Rogue AP detection in RF groups

A rogue AP detection in an RF group is a wireless security feature that

- enables APs in the group to identify unauthorized neighboring APs
- uses beacon and probe-response frames to check for matching authentication elements, and
- automatically reports and records unauthorized devices for network monitoring and response.

After you create an RF group of controllers, you must configure connected access points to detect rogue APs. APs analyze neighbor messages for matching authentication elements. If a match is found, the AP authenticates the frame. If the authentication elements do not match, the AP reports the neighboring AP as rogue, logs its BSSID, and sends the log to the controller or embedded controller.

Secure RF groups

Secure RF groups are a wireless LAN controller feature that

- encrypt radio frequency grouping and RRM message exchanges over a DTLS tunnel
- authenticate controllers using wireless management trust-point certificates during the DTLS handshake, and
- require all participating controllers to belong to the same mobility group.

RF profile configuration recommendation

The RF profile configuration recommendations are:

- Ensure that the country code configuration on both leader and member controllers match.
- RF grouping formation will not form if:
  - The group leader has IPv4 address and the group member has IPv6 address.
  - The group leader has IPv6 address and the group member has IPv4 address.
- Configure the IPv4 address on the group leader if RF grouping occurs between leader and member using IPv6 address.
- We recommend having the same RF profile configurations on the RF group leader and member controllers.
  - Since the RRM algorithms run on the group leader, they refer to the RF profile configurations of the leader controller. For example, additional channels in the member controller's list are not included by the group leader when it assigns a channel to the radio. Similarly, if there is a difference in configuration for DBS channel width between the leader and member controller, the algorithm only refers to the configurations of the group leader.
- For premises with over 20 controllers, we recommend that you have a common (non-default) RF network name for up to 20 controllers. The rest of the controllers can be mapped under different RF network names.
- For better network control, set your controller as static leader.

Examples: RF group configuration

These are examples of RF group name configuration.

```
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 demonstrates how to configure rogue AP sdetection within 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
```

Transmit power control

A transmit power control is an automation algorithm that:

- increases and decreases an access point's power dynamically
- responds to changes in the RF coverage environment, and
- provides enough RF power to achieve the required coverage levels while avoiding channel interference.

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 APs. 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.

Override the TPC algorithm with minimum and maximum transmit power settings

A Transmit Power Control (TPC) minimum and maximum transmit power setting is a wireless network configuration option that

- defines the allowed range of RF transmit powers for APs
- overrides the automatic power adjustment recommendations of the TPC algorithm, and
- applies settings globally to APs through RF profiles.

The TPC (Transmit Power Control) algorithm automatically balances RF power in various environments. Occasionally, site or architectural constraints require manually overriding TPC recommendations. With minimum and maximum power settings, you ensure APs do not exceed or fall below specific transmit powers, regardless of TPC or automatic adjustments or coverage hole detection.

Each AP model and each regulatory domain has its own allowed power levels. The increments vary: Cisco APs use 3 dB increments, but settings can be chosen in 1 dB increments and rounded.

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 from –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point 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 AP will transmit above 11 dBm unless the AP 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 about Allowed Power Level versus Actual Power (in dBm), use the **show ap name <name> config slot <0|1|2|3>** command. This command displays the specific number of power levels, the allowed range of power levels, and the current power level setting on the AP.

Dynamic channel assignment

A dynamic channel assignment (DCA) is a wireless LAN management technique that

- automatically evaluates radio frequency (RF) conditions and network utilization
- dynamically allocates channels among APs to minimize interference and maximize performance, and
- continuously updates channel assignments based on system-wide RF analytics and policies.

Features of DCA

Features of DCA are:

- **Dynamic channel allocation**: DCA dynamically assigns channels to APs to avoid conflicts and interference, improving network capacity and performance. Two adjacent APs on the same channel can cause signal contention or collision. In a collision, data is not received by the AP. For example, reading an e-mail in a café can affect the performance of an AP 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 AP channel assignments to avoid conflict and increase capacity and performance.

- **Channel reuse**: Efficiently reuses channels by assigning the same channel to APs that are physically far apart, maximizing scarce RF resources. In other words, channel 1 is allocated to a different AP far from the café, which is more effective than not using channel 1 altogether.

- **Adjacent channel separation**: The device's DCA capabilities are also useful in minimizing adjacent channel interference between APs.

  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 separated.

Channel assignments

The device examines a variety of real-time RF characteristics to efficiently handle channel assignments.

- AP received energy: The received signal strength measured between each AP and its nearby neighboring AP. Channels are optimized to give you the highest network capacity.
- Noise: Noise can limit signal quality for your devices and APs. Increased noise reduces cell size and degrades user experience. By optimizing channels to avoid noise sources, the device helps you maintain coverage and 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 APs and neighboring wireless networks. Lightweight APs automatically scan all channels to detect interference sources. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the AP 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 APs being on the same channel, but this setup provides better performance than keeping APs on a channel made unusable by interference.

  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 APs are deployed in ways that carry more traffic than other APs, for example, a lobby versus an engineering area. The device can then assign channels to improve the AP 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 AP's transmitted and received packet counts to determine how busy the APs are. New clients avoid an overloaded AP and associate to a new AP. 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 result is optimal channel configuration across three dimensions. APs located on different floors play an important role in your wireless LAN configuration.

RRM startup mode

The RRM startup mode is invoked under these 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 using the **ap dot11 {24ghz | 5ghz | 6ghz} rrm dca restart** command.

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

Dynamic bandwidth selection

Dynamic bandwidth selection is a wireless network algorithm that

- maximizes network throughput by dynamically varying the channel width during operation
- fine-tunes channel assignments by monitoring channel and Base Station Subsystem (BSS) statistics, and
- adapts to changes in network conditions, such as transitions from 11n to 11ac, and variable client mixes.

During upgrades from 11n to 11ac, dynamic bandwidth selection enables a smooth transition between configurations by adjusting channel widths and orientation (such as choosing between 40 MHz and 80 MHz bandwidths) in response to fast-changing wireless statistics.

Limitations for DCA

DCA limitations include the following items.

- DCA supports only 20-MHz channels in the 2.4-GHz band.
- In a Dynamic Frequency Selection (DFS)-enabled AP environment, enable the UNII2 channels option under the DCA channel to allow 100-MHz separation for the dual 5-GHz radios.

- The calculation methods for interference and channel utilization differ between 9120 (and older) AP models and the newer 916x and 917x AP models. The 9120 and older APs estimate interference and channel utilization using Wi-Fi data packets received from non-neighbor Wi-Fi sources during scanning. In contrast, the 916x and 917x APs use the radio chip vendor's hardware-level snapshots to determine channel activity, providing improved accuracy over the older models.
- Use only nonoverlapping channels (1, 6, 11, and others) for reassigning channels to minimize interference.
- Channel change does not require you to shut down the radio.
- The DCA algorithm interval is set to one hour. However, the DCA algorithm always runs at the default interval of 10 minutes. Channel allocation occurs at 10-minute intervals for the first 10 cycles, and channel changes occur every 10 minutes as determined by the DCA algorithm. After these cycles, the DCA algorithm returns to the configured interval.
- Invoking channel update will not result in any immediate changes until the next DCA interval is triggered.
- If DCA or Transmit Power Control (TPC) is turned off on the RF group member, and automatic settings are enabled on the RF group leader, the channel or transmit power on the member changes according to the algorithm run on the RF group leader.

Coverage hole detection and correction

A coverage hole detection and correction algorithm is a wireless LAN management mechanism that

- identifies areas with insufficient radio coverage for reliable performance
- alerts administrators when access points fail to provide adequate coverage, and
- adjusts AP transmit power to mitigate correctable coverage holes.

If clients on a lightweight AP are detected at threshold levels such as RSSI, failed client count, percentage of failed packets, and number of failed packets that are lower than those specified in the RRM configuration, the AP sends a "coverage hole" alert to the device. The alert indicates that clients cannot connect to a usable AP because of poor signal coverage.

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 AP.

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. Increasing downstream transmit power could increase interference in the network.

Cisco AI enhanced RRM

A Cisco AI enhanced RRM is a wireless radio resource management technology that

- applies artificial intelligence and machine learning to optimize RF environments
- operates through distributed data collection from Cisco wireless controllers and cloud-based analytics, and
- automates and adapts RF parameter tuning for Cisco wireless networks.

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.

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

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

- DCA
- TPC
- DBS
- FRA

Cisco AI enhanced RRM supporting releases

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

Table 3: 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

Controller release	Cisco Catalyst Center release	Cisco AI enhanced RRM support
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

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 .

Restrictions

The restrictions for RRM are:

- The maximum number of APs supported in an RF group depends on the capacity of the controller platform acting as the RF group leader. For platform-specific RF-group limits, refer the C9800 Radio Resource Management Deployment Guide.
- 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** affects the 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 like **secure** are not permissible as RF group names.
- 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.

How to configure RRM

Configure neighbor discovery type (GUI)

Configure the Neighbor Discovery Type for your network devices by leveraging the GUI interface.

Use this task to set the Neighbor Discovery Type within the Radio Resource Management settings to enhance the network's ability to detect and manage neighbor devices efficiently.

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 range is from 0 to 100 %. The default is 10 %.
2. **Clients**: The client threshold range is from 1 to 75 clients. The default is 12.
3. **Noise**: The foreign noise threshold range is from –127 dBm to 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 10000000 bps. The default value is 1000000.

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

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 these options:

- **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.

Neighbor discovery for your network devices is complete.

Configure neighbor discovery type (CLI)

Specify how neighbor discovery packets are handled on each radio band.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the neighbor discovery type for the desired radio band.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm ndp-type {protected | transparent}
```

The NDP types are:

- **protected**: Use **protected** to encrypt discovery packets.
- **transparent**: Use **transparent** to send packets as is (default).

Step 3 Return to privileged EXEC mode by ending the configuration mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The neighbor discovery type for the specified band is set.

Configure RF groups

RF groups are configured through either GUI or CLI. You can also configure RF groups through

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.

Configure RF group selection mode (GUI)

Set the RF Group Selection Mode for a wireless controller to manage radio resource management (RRM) and group configuration.

Use this procedure when you need to designate or update the RF Group Selection Mode on your controller using the web interface.

Before you begin

Ensure you have administrator access to the wireless controller GUI.

To configure the RF Group Selection Mode, use the steps in this section:

Procedure

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

Step 2 On the **RRM** page, click the relevant band 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 leader. Controllers managed by Cisco Catalyst Center with AI Enhanced RRM enabled are assigned the group role as remote members regardless of the group mode previously assigned. The **Group Role** field displays **Remote Member**, and the **Group leader** field displays the IP address of the Cisco Catalyst Center.

Step 5 Save the configuration.

The controller applies the selected RF Group Selection Mode to the chosen bands.

Configure RF group selection mode (CLI)

Set the RF group selection mode for specific 802.11 radio bands on a Cisco device using CLI commands.

Use this procedure to configure how access points are grouped for RF management purposes by specifying the RF group selection mode for 2.4 GHz, 5 GHz, or (if supported) 6 GHz bands.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the RF group selection mode for your 802.11 band.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm group-mode {auto | leader | off}
```

- **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 Configure RF group selection mode for 802.11 bands.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm group-mode {auto | leader | off}
```

- **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 4 Exit configuration mode to return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The system applies the selected RF group selection mode to the specified 802.11 band.

Configure an RF group name (CLI)

Set up a radio frequency (RF) group for wireless controllers. This action optimizes radio resource management.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create an RF group. Enter a group name in ASCII format, up to 19 characters long. The name is case sensitive.

Example:

```
Device(config)# wireless rf-network network-name
```

Note
Repeat this procedure for each controller you want to add to the RF group.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

You can also press **Ctrl-Z** to exit global configuration mode.

The RF group is created. Controllers in the group share RF information to optimize radio performance.

```
Device# configure terminal
Device(config)# wireless rf-network network1
Device(config)# end
Device# show network profile 100
```

Configure a secure RF group (CLI)

Set up a secure RF group for optimal wireless device communication and management.

With a secure RF group, your access points coordinate radio resources to improve network performance.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a secure RF group and enable the secure RF group functionality.

Example:

```
Device(config)# wireless rf-network secure
```

Step 3 Exit to privileged EXEC mode.

Example:

```
Device(config)# end
```

Step 4 (Optional) Verify the RF group configuration and statistics for the desired frequency band , such as 2.4 GHz, 5 GHz, or 6 GHz.

Example:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} group
```

The secure RF group is created and operational on the selected wireless controller.

Configure members in an 802.11 static RF group (GUI)

Add controllers to a static RF group. This configuration enables coordinated radio management and optimizes wireless network performance.

When you configure static RF groups, you can manually designate RF group leaders and members. This approach supports predictable behavior and enhances control over radio resource management.

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 these options:

- **Automatic (default)**: Members of an RF group elect a leader to maintain a primary power and channel scheme. The RF grouping algorithm selects the group leader dynamically and ensures continuous leadership. Group leader assignments can change. For example, assignments change if the current leader becomes inoperable or if group members experience significant changes.
- **Leader**: A device as an RF group leader, manually. In this mode, the leader and members are manually configured. Their assignments remain fixed. If a member is unable to join the RF group, the system indicates the reason. The system uses the member's management IP address and system name to request that the member join the leader. The leader attempts to connect with a member every minute if the member did not join during 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**.

The new member is added to the static RF group and joins the manually configured group for radio parameter coordination.

Configure members in an 802.11 static RF group (CLI)

Define APs as members of a static RF group using the CLI, enabling coordinated radio management.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure members in an 802.11 static RF group.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm group-member group_name ip_addr
```

Set the group mode to leader to activate the group member.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

You can also press **Ctrl-Z** to exit global configuration mode.

The AP is added as a member of the 802.11 static RF group.

```
Device# configure terminal
Device(config)# ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1
Device(config)# end
```

Configure transmit power control

•

Configure transmit power (GUI)

Configure transmit power settings for wireless APs.

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 one of these 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 AP attached to the device to exceed this transmit power level. This applies 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 AP would transmit above 11 dBm, unless the AP is configured manually. The range is from –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 APs are transmitting at higher (or lower) than desired power levels. The range is from –80 to –50 dBm.

Increasing this value (between –65 and –50 dBm) causes the APs to operate at higher transmit power rates. Decreasing the value has the opposite effect. In applications with a dense population of APs, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (APs) 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** .

Transmit power settings are updated according to your configuration.

Configure Tx-power control threshold (CLI)

Set the Tx-power control threshold to define the minimum received signal strength at which the device adjusts its transmit power.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the Tx-power control threshold used by RRM for auto power assignment.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm tpc-threshold threshold_value
```

The range is from –80 dBm to –50 dBm.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

You can also press **Ctrl-Z** to exit global configuration mode.

The Tx-power control threshold is updated, enabling the device to adjust its transmit power according to the specified threshold.

```
Device# configure terminal
Device(config)# ap dot11 24ghz rrm tpc-threshold -60
Device(config)# end
```

Configure the Tx-power level (CLI)

Set the transmit power level of the wireless AP to improve wireless coverage and signal strength.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the 802.11 Tx-power level.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm txpower {trans_power_level | auto | max | min
| once}
```

The Tx-power parameters are:

- **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 Configure the 802.11 6-GHz Tx-power level.

Example:

```
Device(config)# ap dot11 6ghz rrm txpower trans_power_level auto
```

The Tx-power parameters are:

- *trans_power_level*: Sets the transmit power level. The range is 1 to 5.
- **auto**: Enables auto-RF.

Note
The 6-GHz band uses constant-PSD instead of constant-EIRP, which allows you to transmit at higher power as the channel width increases. The system derives the power levels based on the configured channel width. At higher power levels between 1 and 3, these power values exceed the limit for legacy rate frames, such as beacon frames. The beacon power does not change at higher levels in the 6-GHz band, unlike in the 2.4-GHz and 5-GHz bands.

Step 4 **end**

Example:

```
Device(config)# end
```

Return to privileged EXEC mode.

Configure 802.11 RRM parameters

-

Configure advanced 802.11 channel assignment parameters (GUI)

Configure the RRM settings to optimize channel assignment for 802.11 wireless networks.

Procedure

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

Step 2 In the **DCA** tab, complete these details:

a) Select 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.

b) 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.

c) 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.

d) 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 APs avoid channels close to foreign APs. By default, this feature is in enabled state.

e) 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 APs that carry a heavier traffic load. By default, this feature is in disabled state.

f) 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.

g) 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.

h) 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.

i) 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 3 The **Auto-RF Channel List** section shows the channels that are currently selected. To select 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 4 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 5 Click **Apply** .

The wireless controller updates 802.11 channel assignments according to your configured parameters.

Configure 802.11 channel assignment parameters (CLI)

Configure DCA and related parameters on 802.11 radios.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure CleanAir event-driven RRM parameters.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel cleanair-event sensitivity {high | low
 | medium}
```

The types of sensitivity are:

- **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 Configure 802.11 6GHz DCA algorithm parameters.

Example:

```
Device(config)# ap dot11 6ghz rrm channel dca {anchor-time <0-23> | global auto | interval
 <0-24> sensitivity {high | low | medium}}
```

The DCA algorithm parameters include:

- **anchor-time**: Configures the anchor time for the DCA. The range is from 0 to 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 Configure the DCA channel bandwidth for all 802.11 radios in the 5-GHz band.

Example:

```
Device(config)# ap dot11 5ghz rrm channel dca chan-width {20 | 40 | 80 | best}
```

The channel bandwidth can be set to 20 MHz, 40 MHz, or 80 MHz, . The default value for channel bandwidth is 20 MHz (80 MHz is the default value for Best). Set the channel bandwidth to Best before configuring the constraints.

Step 5 Configure the maximum channel bandwidth that can be assigned to a channel.

Example:

```
Device(config)# ap dot11 5ghz rrm channel dca chan-width width-max {WIDTH_20MHz | WIDTH_40MHz
 | WIDTH_80MHz |WIDTH_MAX}
```

WIDTH_80MHz assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.

Step 6 Configure the maximum channel bandwidth that can be assigned to a channel.

Example:

```
Device(config)# ap dot11 6ghz rrm channel
dca chan-width width-max {WIDTH_200MHz | WIDTH_40MHz | WIDTH_80MHz | WIDTH_MAX}
```

WIDTH_80MHz assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.

The 802.11 channel assignment parameters are configured.

What to do next

Configure the advanced channel assignment parameters.

Configure the advanced channel assignment parameters (CLI)

Procedure

Step 1 Configure the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel device
```

Step 2 Configure the foreign AP 802.11 interference avoidance in the channel assignment.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel foreign
```

Step 3 Configure the Cisco AP 802.11 load avoidance in the channel assignment.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel load
```

Step 4 Configure noise avoidance in 802.11 channel assignment.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel noise
```

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

You can also press **Ctrl-Z** to exit global configuration mode.

The 802.11 advanced channel assignment parameters are configured.

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel noise
  Device(config)# end
```

Configure 802.11 coverage hole detection (GUI)

Enable 802.11 coverage hole detection to optimize wireless radio coverage and identify areas with inadequate connectivity.

Use this task when you want to detect and troubleshoot Wi-Fi coverage gaps on 6 GHz, 5 GHz, or 2.4 GHz radio bands in your wireless network.

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 the **Coverage** tab and complete these steps:

a) To enable coverage hole detection, check the **Enable Coverage Hole Detection** check box.

b) In the **Data Packet Count** field, enter the number of data packets.

c) In the **Data Packet Percentage** field, enter the percentage of data packets.

d) In the **Data RSSI Threshold** field, enter the actual value in dBm. The range is from –60 dBm to –90 dBm. The default value is –80 dBm.

e) In the **Voice Packet Count** field, enter the number of voice data packets.

f) In the **Voice Packet Percentage** field, enter the percentage of voice data packets.

g) In the **Voice RSSI Threshold** field, enter the actual value in dBm. The range is from –60 dBm to –90 dBm. The default value is –80 dBm.

h) 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. The range is from 1 to 75, and the default value is 3.

i) 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. The range is from 0 to 100%, and the default value is 25%.

Step 3 Click **Apply**.

Your configuration is saved and the system begins monitoring for coverage holes based on the specified parameters.

Configure 802.11 coverage hole detection (CLI)

Set up coverage hole detection for your wireless network.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the 802.11 6 GHz coverage hole detection for data packets.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm coverage data {fail-percentage |
packet-count} value
```

The attributes for the data packets are:

- **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 percent.
- **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.

Step 3 Configure the 802.11 AP coverage exception level as a percentage that ranges from 0 to 100 percent.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm coverage exception global exception-level
```

Step 4 Set the minimum exception level for AP clients.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm coverage level global cli_min exception level
```

The value range is from 1 to 75 clients.

Step 5 Configure the 802.11 6 GHz coverage hole detection for voice packets.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm coverage voice {fail-percentage |
packet-count} value
```

The attributes for voice packets are:

- **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 percent.
- **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.

Step 6 Return to privileged EXEC mode to complete configuration.

Example:

```
Device(config)# end
```

ress **Ctrl-Z** to exit global configuration mode.

After you configure coverage hole detection thresholds, the wireless APs monitor your network and send alerts about coverage gaps.

```
Device# configure terminal
Device(config)# ap dot11 24ghz rrm coverage data fail-percentage 60
Device(config)# ap dot11 6ghz rrm coverage data fail-percentage 60
Device(config)# ap dot11 24ghz rrm coverage exception global 50
Device(config)# ap dot11 24ghz rrm coverage level global 10
Device(config)# ap dot11 24ghz rrm coverage voice packet-count 10
Device(config)# ap dot11 6ghz rrm coverage voice packet-count 10
Device(config)# end
```

Configure 802.11 event logging (CLI)

Enable and customize event logging for 802.11 wireless network parameters.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure event-logging for various parameters.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm logging {channel | coverage | foreign |
 load | noise | performance | txpower}
```

The event-logging parameters include:

- **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 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

You can also press **Ctrl-Z** to exit global configuration mode.

You have enabled 802.11 event logging for the specified parameters.

```
Device# configure terminal

Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm logging {channel | coverage | foreign |
 load | noise | performance | txpower}
Device(config)# end
```

Configure 802.11 statistics monitoring (GUI)

Enable and customize radio statistics monitoring intervals for APs.

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 3600 secs)** section:

a) To configure the 802.11 noise measurement interval (channel scan interval), set the **AP Noise Interval**. The valid range is from 60 to 3,600 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 3,600 seconds.

c) To configure the 802.11 coverage measurement interval, set the **AP Coverage Interval**. The valid range is from 60 to 3,600 seconds.

d) To configure the 802.11 load measurement, set the **AP Load Interval**. The valid range is from 60 to 3,600 seconds.

Step 3 Click **Apply**.

802.11 statistics monitoring intervals are applied to the selected radios.

Configure 802.11 statistics monitoring (CLI)

Enable or customize the monitoring of 802.11 statistics on wireless APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Set the 802.11 monitoring channel-list for parameters such as noise/interference/rogue.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor channel-list {all | country |
dca}
```

The channel list parameters include:

- **all**: Monitors all channels.
- **country**: Monitor channels used in configured country code.
- **dca**: Monitor channels used by dynamic channel assignment.

Step 3 Configure the 802.11 coverage measurement interval in seconds, which ranges from 60 to 3,600.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor coverage interval
```

Step 4 Configure the 802.11 load measurement interval in seconds, which ranges from 60 to 3,600.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor load interval
```

Step 5 Configure the 802.11 noise measurement interval (channel scan interval) in seconds, which ranges from 60 to 3,600.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor noise interval
```

Step 6 Configure the 802.11 signal measurement interval (neighbor packet frequency) in seconds, which ranges from 60 to 3,600.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor signal interval
```

Step 7 Configure the 802.11 RRM Neighbor Discovery RSSI normalization.

Example:

```
Device(config)#ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor rssi-normalization
```

The system applies your 802.11 statistics monitoring settings to the APs.

```
Device# configure terminal
Device(config)# ap dot11 6ghz rrm monitor channel-list all
Device(config)# ap dot11 6ghz rrm monitor coverage 600
```

```
Device(config)# ap dot11 6ghz rrm monitor load 180
Device(config)# ap dot11 6ghz rrm monitor noise 360
Device(config)# ap dot11 6ghz rrm monitor signal 480
Device(config)# ap dot11 6ghz rrm monitor rssi-normalization
```

Configure the 802.11 performance profile (GUI)

Define radio frequency parameters to optimize AP performance in 802.11 networks.

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, which ranges from 0 to 100 percent.

b) In the **Clients** field, enter the threshold value for 802.11 Cisco AP clients, which ranges from 1 to 75 clients.

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

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

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

The 802.11 performance profile is applied to the selected APs.

Configure the 802.11 performance profile (CLI)

Configure threshold values for 802.11 performance parameters, including clients, interference, noise, throughput, and RF utilization, on Cisco APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Set the threshold value for 802.11 Cisco AP clients, which ranges from 1 to 75 clients.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm profile clients cli_threshold_value
```

Step 3 Set the threshold value for 802.11 foreign interference, which ranges from 0 to 100 percent.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm profile foreign int_threshold_value
```

Step 4 Set the threshold value for 802.11 foreign noise, which ranges from –127 to 0 dBm.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm profile noise for_noise_threshold_value
```

Step 5 Enable performance profiles.

Example:

```
Device(config)# ap dot11 6ghz rrm profile customize
```

Step 6 Set the threshold value for 802.11 Cisco AP throughput, which ranges from 1000 to 10000000 bytes per second.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm profile throughput
throughput_threshold_value
```

Step 7 Set the threshold value for 802.11 RF utilization, which ranges from 0 to 100 percent.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm profile utilization rf_util_threshold_value
```

Step 8 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The AP's performance profile is updated with your specified threshold values, enabling automated monitoring and adjustment of wireless network conditions according to configured criteria.

```
Device# configure terminal
Device(config)# ap dot11 24ghz rrm profile clients 20
Device(config)# ap dot11 24ghz rrm profile foreign 50
Device(config)# ap dot11 24ghz rrm profile noise -65

Device(config)# ap dot11 6ghz rrm profile customize
Device(config)# ap dot11 24ghz rrm profile throughput 10000
Device(config)# ap dot11 24ghz rrm profile utilization 75
Device(config)# end
```

Configure advanced 802.11 RRM

-

Enable channel assignment (GUI)

To optimize wireless performance, assign device radio channels either automatically or manually.

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**:

- **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**.

Dynamic channel assignment is enabled based on your selection. You can configure radios to use automatic or manual channel allocation.

Enable channel assignment (CLI)

To optimize radio resource allocation, assign wireless channels to 802.11 APs.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device# enable
```

Step 2 Enable the 802.11 channel selection update for each AP.

Example:

```
Device# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel-update
```

Note
After enabling the feature, the DCA algorithm assigns a token for channel assignment.

The system applies the DCA algorithm to update wireless channel assignments on all APs for the specified frequency.

```
Device# enable
Device# ap dot11 24ghz rrm channel-update
```

Restart DCA operation

To restore optimal channel allocation for wireless radios, restart the Dynamic Channel Assignment (DCA).

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device# enable
```

Step 2 Restart the DCA cycle for the 802.11 radio.

Example:

```
Device# ap dot11 {24ghz | 5ghz  | 6ghz} rrm dca restart
```

The DCA process restarts on the wireless device.

```
Device# enable
Device# ap dot11 24ghz rrm dca restart
```

Update power assignment parameters (GUI)

Change the transmit power assignment settings for your AP to optimize wireless coverage.

Procedure

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

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

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

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

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

The system applies the updated transmit power parameters to your selected AP.

Update power assignment parameters (CLI)

Adjust the wireless transmit power settings for APs to optimize coverage and performance.

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Device# enable
```

Step 2 Update the 802.11 6 GHz transmit power for every AP.

Example:

```
Device# ap dot11 {24ghz | 5ghz | 6ghz} rrm txpower update
```

The system updates the transmit power configuration for the specified APs.

```
Device# enable
Device# ap dot11 24ghz rrm txpower update
Device# ap dot11 6ghz rrm txpower update
```

Monitor RRM parameters and RF group status

Monitor RRM parameters

Provide a quick reference to the commands used for monitoring Radio Resource Management (RRM) parameters, enabling users to efficiently assess and troubleshoot wireless network performance.

Table 4: Commands for monitoring Radio Resource Management

Commands	Description
show ap dot11 24ghz channel	Displays the configuration and statistics of the 802.11b monitoring.
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. nnn
show ap dot11 24ghz profile	Displays 802.11b profiling information for all APs.
show ap dot11 24ghz summary	Displays the configuration and statistics of the 802.11a 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 APs.

Commands	Description
show ap dot11 5ghz summary	Displays the configuration and statistics of the 802.11a APs.
show ap dot11 5ghz txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Verify RF group status

This section describes the new commands for RF group status.

These commands are used to verify RF group status on the .

This table lists the commands for verifying aggressive load balancing.

Table 5: Aggressive load balancing verification commands

Command	Purpose
show ap dot11 5ghz group	Displays the controller name that is the group leader for the 802.11a RF network.
show ap dot11 24ghz group	Displays the controller name that is the group leader for the 802.11b/g RF network.
show ap dot11 6ghz group	Displays the controller name that is the 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 this 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         192.0.2.188     N/A
```

Event-Driven Radio Resource Management

A Event-Driven Radio Resource Management (ED-RRM) feature is a radio frequency management solution that

- continuously monitors air quality metrics

- automatically triggers channel changes when interference exceeds a set threshold, and
- blocks affected channels for a specified duration to prevent immediate reselection.

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 AP. 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 AP detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active.

Configure ED-RRM on the controller (CLI)

Configure Event-Driven Radio Resource Management (ED-RRM) on the controller using CLI commands.

Trigger spectrum event-driven RRM to run when a Cisco CleanAir-enabled AP detects a significant level of interference by entering these commands.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure CleanAir driven RRM parameters for the 802.11 APs.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel cleanair-event
```

Step 3 Configure CleanAir driven RRM sensitivity for the 802.11 APs.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel cleanair-event sensitivity {low
 | medium | high | custom}
```

Default selection is Medium.

Step 4 Trigger the ED-RRM event at the set threshold value.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel cleanair-event custom-threshold
 custom-threshold-value
```

The custom threshold range is from 1 to 99.

Step 5 Enable rogue contribution.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel cleanair-event rogue-contribution
```

Step 6 Configure threshold value for rogue contribution.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz | 6ghz} rrm channel cleanair-event rogue-contribution
 duty-cycle thresholdvalue
```

The range is from 1 to 99, with 80 as the default.

Step 7 Save your changes.

Example:

```
Device# write memory
```

Step 8 (Optional) Verify the CleanAir configuration for the 802.11a/n/ac or 802.11b/g/n network.

Example:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz}cleanair config
```

The output is displayed.

```
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
```

The Event-Driven Radio Resource Management (ED-RRM) on the controller is configured.

Rogue detection - rogue channel width

A rogue detection configuration is a security measure that

- allows specifying channel width and band for detecting unauthorized APs, and
- filters rogue APs based on matching channel width criteria and band.

The **condition chan-width** command is introduced in Cisco IOS XE Dublin 17.12.1 allows you to set the minimum or maximum channel width for rogue detection.

Configure rogue channel width (CLI)

Complete this task to configure rogue channel width.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create or enable a rule.

Example:

```
Device(config)# wireless wps rogue rule rule-name priority priority
```

Step 3 Configure channel width and band for rogue detection.

Example:

```
Device(config-rule)# condition chan-width {160MHz | 20MHz | 40MHz | 80MHz} band {24ghz |
5ghz | 6ghz}
```

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 Step 4, 5, 6, or 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 (Optional) Classify devices matching this rule as friendly.

Example:

```
Device(config-rule)# classify friendly state {alert | external | internal}
```

The options are:

- **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 (Optional) Classify devices matching this rule as malicious.

Example:

```
Device(config-rule)# classify malicious state {alert | contained}
```

The options are:

- **alert**: Sets the malicious rogue AP to alert mode.
- **contained**: Contains the rogue AP.

Step 7 (Optional) Classify devices matching this rule as custom.

Example:

```
Device(config-rule)# classify custom severity-score severity-score [name name] state {alert
 | contained}
```

Here the options are:

- *severity-score* : Custom classification severity score. The range is from 1 to 100.
- **name**: Defines the name for custom classification.
- *name* : Specifies the custom classification name.
- **state**: Defines the final state if rule is matched.
- **alert**: Sets the rogue AP to alert mode.
- **contained**: Contains the rogue AP.

Step 8 Ignore the devices matching this rule.

Example:

```
Device(config-rule)# classify delete
```

Step 9 Return to privileged EXEC mode.

Example:

```
Device(config-rule)# end
```

The rogue channel width is configured.

```
Device# configure terminal
                Device(config)# wireless wps rogue rule 1 priority 1
                Device(config-rule)# condition chan-width 20MHz band 5ghz
                Device(config-rule)# classify friendly state internal
                Device(config-rule)# classify malicious state alert
                Device(config-rule)# classify custom severity-score 12 name rule1 state
alert
                Device(config-rule)# classify delete
                Device(config-rule)# end
```

Configure rogue classification rules (GUI)

Complete this task to configure rogue classification rules.

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 with these steps:

a) Click **Add**.

b) In the **Add Rogue AP Rule** window, 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 these options to classify rogue APs matching this rule:

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

d) From the **State** drop-down list, configure the state of the rogue AP. 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 using these steps:

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 these options to classify rogue APs 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 these options:

- **Match All**: The detected rogue AP must meet all of the conditions specified by the rule for the rule to be matched and the rogue AP to adopt the classification type of the rule.
- **Match Any**: The detected rogue AP must meet any of the conditions specified by the rule for the rule to be matched and the rogue AP 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 conditions that the rogue AP must meet:

- **None**: No condition is set for rogue AP detection.
- **client-count**: Condition requires that a minimum number of clients be associated to the rogue AP. For example, if the number of clients associated to the rogue AP is greater than or equal to the configured value, then the AP can be classified as malicious. If you choose this option, enter the minimum number of clients to be associated with the rogue AP 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 AP 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 AP's advertised WLAN does not have encryption enabled. If a rogue AP 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 AP'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 AP have a minimum received signal strength indication (RSSI) value. For example, if the rogue AP has an RSSI that is greater than the configured value, then the AP 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 AP use the specified radio spectrum channel width for the specified radio band, as defined. 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 AP 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 AP 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**.

The rogue classification rules are configured.

Verify rogue channel width

To view channel width and band information of a classification rule, use these 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
```

Rogue detection - rogue channel width

A rogue detection configuration is a security measure that

- allows specifying channel width and band for detecting unauthorized APs, and
- filters rogue APs based on matching channel width criteria and band.

The **condition chan-width** command is introduced in Cisco IOS XE Dublin 17.12.1 allows you to set the minimum or maximum channel width for rogue detection.

Configure rogue channel width (CLI)

Complete this task to configure rogue channel width.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create or enable a rule.

Example:

```
Device(config)# wireless wps rogue rule rule-name priority priority
```

Step 3 Configure channel width and band for rogue detection.

Example:

```
Device(config-rule)# condition chan-width {160MHz | 20MHz | 40MHz | 80MHz} band {24ghz |
5ghz | 6ghz}
```

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 Step 4, 5, 6, or 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 (Optional) Classify devices matching this rule as friendly.

Example:

```
Device(config-rule)# classify friendly state {alert | external | internal}
```

The options are:

- **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 (Optional) Classify devices matching this rule as malicious.

Example:

```
Device(config-rule)# classify malicious state {alert | contained}
```

The options are:

- **alert**: Sets the malicious rogue AP to alert mode.
- **contained**: Contains the rogue AP.

Step 7 (Optional) Classify devices matching this rule as custom.

Example:

```
Device(config-rule)# classify custom severity-score severity-score [name name] state {alert
 | contained}
```

Here the options are:

- *severity-score* : Custom classification severity score. The range is from 1 to 100.
- **name**: Defines the name for custom classification.
- *name* : Specifies the custom classification name.
- **state**: Defines the final state if rule is matched.
- **alert**: Sets the rogue AP to alert mode.
- **contained**: Contains the rogue AP.

Step 8 Ignore the devices matching this rule.

Example:

```
Device(config-rule)# classify delete
```

Step 9 Return to privileged EXEC mode.

Example:

```
Device(config-rule)# end
```

The rogue channel width is configured.

```
Device# configure terminal
                Device(config)# wireless wps rogue rule 1 priority 1
                Device(config-rule)# condition chan-width 20MHz band 5ghz
                Device(config-rule)# classify friendly state internal
                Device(config-rule)# classify malicious state alert
                Device(config-rule)# classify custom severity-score 12 name rule1 state
alert
                Device(config-rule)# classify delete
                Device(config-rule)# end
```

Configure rogue classification rules (GUI)

Complete this task to configure rogue classification rules.

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 with these steps:

a) Click **Add**.

b) In the **Add Rogue AP Rule** window, 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 these options to classify rogue APs matching this rule:

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

d) From the **State** drop-down list, configure the state of the rogue AP. 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 using these steps:

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 these options to classify rogue APs 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 these options:

- **Match All**: The detected rogue AP must meet all of the conditions specified by the rule for the rule to be matched and the rogue AP to adopt the classification type of the rule.
- **Match Any**: The detected rogue AP must meet any of the conditions specified by the rule for the rule to be matched and the rogue AP 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 conditions that the rogue AP must meet:

- **None**: No condition is set for rogue AP detection.
- **client-count**: Condition requires that a minimum number of clients be associated to the rogue AP. For example, if the number of clients associated to the rogue AP is greater than or equal to the configured value, then the AP can be classified as malicious. If you choose this option, enter the minimum number of clients to be associated with the rogue AP 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 AP 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 AP's advertised WLAN does not have encryption enabled. If a rogue AP 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 AP'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 AP have a minimum received signal strength indication (RSSI) value. For example, if the rogue AP has an RSSI that is greater than the configured value, then the AP 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 AP use the specified radio spectrum channel width for the specified radio band, as defined. 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 AP 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 AP 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**.

The rogue classification rules are configured.

Verify rogue channel width

To view channel width and band information of a classification rule, use these 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
```