Radio Resource Management

- Radio resource management, on page 1
- Restrictions, on page 6
- How to Configure RRM, on page 6
- Monitoring RRM Parameters and RF Group Status, on page 17
- Examples: RF group configuration, on page 19
- Event-Driven Radio Resource Management , on page 19
- Rogue PMF containment, on page 20
- Enable rogue PMF containment, on page 21
- Verify PMF containment, on page 22
- Rogue detection - rogue channel width, on page 23
- Configure rogue channel width (CLI), on page 23
- Configure rogue classification rules (GUI), on page 25
- Verify rogue channel width, on page 27

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

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.

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.

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.

Restrictions

The restrictions for RRM are:

- 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.
- 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 (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} 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.

Configuring Transmit Power Control

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 **end**

Example:

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

Return to privileged EXEC mode.

Configuring 802.11 RRM 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 DCA algorithm parameters for the 802.11 band.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} rrm channel dca {add channel-number | anchor-time
| global {auto | once} | interval | min-metric | remove channel-number | sensitivity {high
 | low | medium}}
```

The DCA algorithm parameters include:

- : Enter a channel number to be added to the DCA list.
- **anchor-time**: Configures the anchor time for DCA. The range is from 0 to 23 hours.
- **global**: Configures the DCA mode for all 802.11 Cisco APs.
  - **auto**: Enables auto-RF.
  - **once**: Enables auto-RF only once.
- **interval**: Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours, and the default value 0 denotes 10 minutes.
- **min-metric**: Configures the DCA minimum RSSI energy metric. The range is from -100 to -60.
- **sensitivity**: Configures the DCA sensitivity level to changes in the environment.
  - **high**: Specifies the most sensitivity.
  - **low**: Specifies the least sensitivity.
  - **medium**: Specifies medium sensitivity.

Step 4 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}
```

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.

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 (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 coverage hole detection for data packets.

Example:

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

The attributes for the data packets are:

- **fail-percentage**: Configures the 802.11 coverage failure rate threshold for uplink data packets as a percentage that ranges from 1 to 100 percent.
- **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.
- **rssi-threshold**: Configures the 802.11 minimum receive coverage level for data packets that range from –90 dBm to –60 dBm.

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 coverage hole detection for voice packets.

Example:

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

The attributes for voice packets are:

- **fail-percentage**: Configures the 802.11 coverage failure rate threshold for uplink voice packets as a percentage that ranges from 1 to 100 percent.
- **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.
- **rssi-threshold**: Configures the 802.11 minimum receive coverage level for voice packets that range from –90 dBm to –60 dBm.

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)# 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} 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} rrm logging {channel | coverage | foreign | load |
 noise | performance | txpower}

Device(config)# end
```

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} 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} 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} 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} 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} rrm monitor signal interval
```

Step 7 Return to privileged EXEC mode.

Example:

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

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

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

```
Device# configure terminal
Device(config)# ap dot11 24ghz rrm monitor channel-list all
Device(config)# ap dot11 24ghz rrm monitor coverage 600
Device(config)# ap dot11 24ghz rrm monitor load 180
Device(config)# ap dot11 24ghz rrm monitor noise 360
Device(config)# ap dot11 24ghz rrm monitor signal 480
Device(config)# end
```

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 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} rrm profile throughput throughput_threshold_value
```

Step 6 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 7 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 24ghz rrm profile throughput 10000

Device(config)# ap dot11 24ghz rrm profile throughput 10000
```

```
Device(config)# ap dot11 24ghz rrm profile utilization 75
Device(config)# end
```

Configuring Advanced 802.11 RRM

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} 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 } rrm dca restart
```

The DCA process restarts on the wireless device.

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

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 transmit power for each of the APs.

Example:

```
Device# ap dot11 {24ghz | 5ghz} 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
```

Configuring Rogue Access Point Detection in RF Groups

Configure rogue AP detection in RF groups (CLI)

Enable detection of rogue APs within RF groups on the controllers.

Before you begin

Ensure that you configure each controller in the RF group with the same RF group name.

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

Procedure

Step 1 Perform this step for each AP connected to the controller.

Example:

Step 2 Return to privileged EXEC mode to continue configuration.

Example:

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

Press **Ctrl-Z** to exit global configuration mode as an alternative.

Step 3 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 4 Enable rogue AP detection.

Example:

```
Device(config)# wireless wps ap-authentication
```

Step 5 Set a threshold value for rogue AP alarms.

Example:

```
Device(config)# wireless wps ap-authentication threshold value
```

The system generates an alarm when the threshold value (the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

The threshold ranges from 1 to 255. The default value is 1. Set a higher threshold value to avoid false alarms.

Note
Enable rogue AP detection and set the threshold value on every controller in the RF group.

APs on any controller with rogue detection disabled are reported as rogues.

The system enables rogue AP detection on all APs in the RF group. Alarms are triggered when the configured threshold for invalid authentication frames is met or exceeded within the detection period.

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

Monitoring 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 2: 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.
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 3: 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.

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

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.

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.

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

Rogue PMF containment

Rogue PMF containment is a wireless security feature that

- uses 802.11w Protected Management Frames (PMF) to contain rogue APs and clients

- operates on centrally switched WLANs when the radio channel of the detecting AP matches the rogue AP's channel, and
- activates only when certain mode and channel conditions are met to secure the network against unauthorized devices.

Feature history

Table 4: Feature history table for rogue PMF containment

Feature name	Release information	Feature description
Rogue PMF containment	Cisco IOS XE 17.12.1	Starting with Cisco IOS XE Dublin 17.12.1, the controller contains a rogue AP with 802.11w Protected Management Frame (PMF) on centrally switched wireless LANs. Containment occurs if the client-serving radio channel of a rogue-detecting AP matches the channel of the corresponding rogue AP.

Operational scenarios

PMF containment occurs in these scenarios:

- You can use PMF containment only in the local mode.
- You can perform PMF containment only for rogue clients that have not joined a rogue AP.
- You can use PMF containment only if a rogue-detecting AP shares the same primary channel with a rogue client.
- You cannot use PMF containment on DFS channels, even if a DFS channel serves as the client-serving channel.
- PMF containment works only if at least one WLAN operates on the serving radio.

For information about APs that support the Rogue PMF Containment feature, see Cisco AP Feature Matrix.

Enable rogue PMF containment

Enable PMF containment to protect your wireless network from rogue APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile and enter AP profile configuration mode.

Example:

```
Device(config)# ap profile ap-profile
```

Step 3 Enable PMF-denial rogue AP containment.

Example:

```
Device(config-ap-profile)# rogue detection containment pmf-denial
```

Step 4 Enable PMF-denial type deauthentication rogue AP containment.

Example:

```
Device(config-pmf-denial)# pmf-deauth
```

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

Rogue AP PMF containment is enabled for the specified AP profile.

```
Device# configure terminal
Device(config)# ap profile pmf-ap-profile
Device(config-ap-profile)# rogue detection containment pmf-denial
Device(config-pmf-denial)# pmf-deauth
Device(config-ap-profile)# end
```

Verify PMF containment

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

To view the summary of containment details for all AP radios, use this command

```
Device# show wireless wps rogue containment summary

Rogue Containment activities for each managed AP

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

To verify the rogue statistics, use this command:

```
Device# show wireless wps rogue stats
.
.
.
 States
  Alert                         : 256
  Internal                      : 0
  External                      : 0
```

```
  Contained                     : 1
  Containment-pending           : 0
  Threat                        : 0
  Pending                       : 0
Rogue Clients
  Total/Max Scale               : 20/16000
  Contained                     : 0
  Containment-pending           : 0
.
.
.
```

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
```