Configuring Radio Resource Management

Finding Feature Information

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

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

Prerequisites for Configuring Radio Resource Management

The Switch should be configured as a mobility controller and not a mobility anchor to configure radio resource management. It may require dynamic channel assignment functionality for the home APs to be supported.

Restrictions for Radio Resource Management

The number of APs in a RF-group is limited to 500.

If a 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.

Information About Radio Resource Management

The Radio Resource Management (RRM) software embedded in the switch acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables switches to continually monitor their associated lightweight access points for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference—The amount of traffic coming from other 802.11 sources.
- Noise—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage—The received signal strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- Other —The number of nearby access points.

RRM performs these functions:

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

Radio Resource Monitoring

RRM automatically detects and configures new switches and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points go “off-channel” for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presence of voice traffic (in the last 100 ms), the access points defer off-channel measurements.

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

Transmit Power Control

The switch dynamically controls access point transmit power based on real-time wireless LAN conditions. Typically in TPCv1, power can be kept low to gain extra capacity and reduce interference.

The transmit power control (TPC) algorithm both increases and decreases an access point’s power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce

interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes, enter the maximum and minimum transmit power used by RRM on the Tx Power Control page. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the switch to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually.

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading e-mail in a café affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Switches can dynamically allocate access point channel assignments to avoid conflict and to increase capacity and performance. Channels are “reused” to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The switch’s dynamic channel assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mbps. By effectively reassigning channels, the switch keeps adjacent channels separated.

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

The switch examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- Access point received energy—The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.
- Noise—Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the switch can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.
- 802.11 Interference—Interference is any 802.11 traffic that is not part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the switch. Using the RRM algorithms, the switch may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

  In addition, if other wireless networks are present, the switch 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 switch may choose to avoid this channel. In very dense deployments in which all nonoverlapping channels are occupied, the switch does its best, but you must consider RF density when setting expectations.
- Utilization—When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points (for example, a lobby versus an engineering area). The switch can then assign channels to improve the access point with the worst performance reported.
- Load—The load is taken into account when changing the channel structure to minimize the impact on clients currently in the wireless LAN. This metric keeps track of every access point's transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This parameter is disabled by default.

The switch combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

Note Radios using 40-MHz channels in the 2.4-GHz band are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

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

RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a "coverage hole" alert to the switch. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The switch discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the switch mitigates the coverage hole by increasing the transmit power level for that specific access point. The switch does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

How to Configure RRM

Configuring Advanced RRM CCX Parameters

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval* **Example:** `Switch(config)# ap dot11 24ghz rrm ccx location-measurement 15`	Configures the interval for 802.11 CCX client location measurements. The range is from 10 to 32400 seconds.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring Advanced 802.11 Channel Assignment Parameters

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz	5ghz rrm channel cleanair-event**{**high	low	medium**} **Example:** `Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures cleanair event-driven RRM parameters. • **High–** Specifies the most sensitivity to non-WiFi interference as indicated by the air quality (AQ) value. • **Low–** Specifies the least sensitivity to non-WiFi interference as indicated by the AQ value. • **Medium–** Specifies medium sensitivity to non-WiFi interference as indicated by the AQ value.
Step 3	**ap dot11 24ghz	5ghz rrm channel dca**{*channel number*| **anchor-time	global**{**auto| once**}| **interval	min-metric	sensitivity**{**high	low	medium**}} **Example:** `Switch(config)#ap dot11 24ghz rrm channel dca interval 2`	Configures dynamic channel assignment (DCA) algorithm parameters for the 802.11 band. • ***<1-14>–*** Enter a channel number to be added to the DCA list. • **anchor-time–** Configures the anchor time for the DCA. The range is between 0 and 23 hours. • **global–** Configures the DCA mode for all 802.11 Cisco APs. ◦ **auto–** Enables auto-RF. ◦ **once–** Enables auto-RF only once.

	Command or Action	Purpose
		• **interval–** Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes. • **min-metric–** Configures the DCA minimum RSSI energy metric. The range is between -100 and -60. • **sensitivity–** Configures the DCA sensitivity level to changes in the environment. ◦ **high–** Specifies the most sensitivity. ◦ **low–** Specifies the least sensitivity. ◦ **medium–** Specifies medium sensitivity.
Step 4	**ap dot11 24ghz | 5ghz rrm channel device** **Example:** `Switch(config)#ap dot11 24ghz rrm channel device`	Configures the persistent non-WiFi device avoidance in the 802.11 channel assignment.
Step 5	**ap dot11 24ghz | 5ghz rrm channel foreign** **Example:** `Switch(config)#ap dot11 24ghz rrm channel foreign`	Configures the foreign AP 802.11 interference avoidance in the channel assignment.
Step 6	**ap dot11 24ghz | 5ghz rrm channel load** **Example:** `Switch(config)#ap dot11 24ghz rrm channel load`	Configures the Cisco AP 802.11 load avoidance in the channel assignment.
Step 7	**ap dot11 24ghz | 5ghz rrm channel noise** **Example:** `Switch(config)#ap dot11 24ghz rrm channel noise`	Configures the 802.11 noise avoidance in the channel assignment.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring 802.11 Coverage Hole Detection

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} **Example:** `Switch(config)#ap dot11 24ghz rrm coverage data fail-percentage 90`	Configures the 802.11 coverage hole detection for data packets. • **fail-percentage—** Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%. • **packet-count—** Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255. • **rssi-threshold—** Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.
Step 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level* **Example:** `Switch(config)#ap dot11 24ghz rrm coverage exception global 50`	Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level* **Example:** `Switch(config)#ap dot11 24ghz rrm coverage level global 10`	Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.

	Command or Action	Purpose
Step 5	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} **Example:** `Switch(config)#ap dot11 24ghz rrm coverage voice packet-count 200`	Configures the 802.11 coverage hole detection for voice packets. • **fail-percentage—** Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%. • **packet-count—** Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255. • **rssi-threshold—** Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring Members in a 802.11 Static RF Group

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* **Example:** `Switch(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	Configures members in a 802.11 static RF group. The group mode should be set as leader for the group member to be active.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring RF Group Selection Mode

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring 802.11 Event Logging

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Configuring 802.11 Statistics Monitoring

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} **Example:** `Switch(config)#ap dot11 24ghz rrm monitor channel-list all`	Sets the 802.11 monitoring channel-list for parameters such as noise/interference/rogue. • **all—** Monitors all channels • **country—** Monitor channels used in configured country code • **dca—** Monitor channels used by dynamic channel assignment
Step 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor coverage 600`	Configures the 802.11 coverage measurement interval in seconds that ranges from 60 to 3600.
Step 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor load 180`	Configures the 802.11 load measurement interval in seconds that ranges from 60 to 3600.

	Command or Action	Purpose
Step 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor noise 360`	Configures the 802.11 noise measurement interval (channel scan interval) in seconds that ranges from 60 to 3600.
Step 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor signal 480`	Configures the 802.11 signal measurement interval (neighbor packet frequency) in seconds that ranges from 60 to 3600.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring Neighbor Discovery Type

SUMMARY STEPS

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

DETAILED STEPS

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

Step 2	**ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
	
	Example:
	
	`Switch(config)#ap dot11 24ghz rrm ndp-type protected`
	
	`Switch(config)#ap dot11 24ghz rrm ndp-type transparent`
		Configures the neighbor discovery type.
		• **protected—** Sets the neighbor discover type to protected.
		• **transparent—** Sets the neighbor discover type to transparent.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring the 802.11 Performance Profile

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile clients 20`	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.
Step 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile foreign 50`	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.

	Command or Action	Purpose
Step 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile noise -10`	Sets the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.
Step 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile throughput 10000`	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.
Step 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile utilization 50`	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring the Tx-Power Control Threshold

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring the Tx-Power Level

SUMMARY STEPS

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

DETAILED STEPS

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

Monitoring RRM Parameters

Table 1: Commands for monitoring Radio Resource Management

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

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

Additional References

Related Documents

Related Topic	Document Title
RRM commands and their details	*RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

MIBs

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

Technical Assistance

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

Consolidated Platform Configuration Guide for Wireless Technologies, Cisco IOS XE 3SE (Catalyst 3850 Switches)