
# Configuring Radio Resource Management

This chapter describes radio resource management (RRM) and explains how to configure it on the controllers. It contains these sections:

# Overview of Radio Resource Management

The radio resource management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables controllers 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.

Using this information, RRM can periodically reconfigure the 802.11 RF network for best efficiency. To do this, 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 controllers 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. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

## Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points’ transmit power according to how the access points are seen by their third strongest neighbor.

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 will seek 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, explained below. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

**Note** See Step 7 on page 11-31 for an explanation of the transmit power levels.

# Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In the case of a collision, data is simply 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. Controllers address this problem by dynamically allocating 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 controller’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 controller keeps adjacent channels separated, thereby avoiding this problem.

The controller examines a variety of real-time RF characteristics to efficiently handle channel assignments. These include:

- **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 controller 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 controller. Using the RRM algorithms, the controller 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 controller 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 controller

may choose to avoid this channel. In very dense deployments in which all non-overlapping channels are occupied, the controller 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 controller can then assign channels to improve the access point with the worst performance (and therefore utilization) reported.
- **Load**—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 controller 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.

In controller software releases prior to 5.1, only radios using 20-MHz channels are supported by DCA. In controller software release 5.1 or later, DCA is extended to support 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels). In controller software release 5.1 or later, you can choose between DCA working at 20 or 40 MHz.

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

# Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm is designed to 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 controller. 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 controller discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the controller mitigates the coverage hole by increasing the transmit power level for that specific access point. The controller 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 is not a remedy for poor upstream performance and might increase interference in the network.

**Note** While transmit power control and DCA can operate in multi-controller environments (based on RF domains), coverage hole detection is performed on a per-controller basis. In controller software release 5.2 or later, you can disable coverage hole detection on a per-WLAN basis. See the "Disabling Coverage Hole Detection per WLAN" section on page 6-65 for more information.

## RRM Benefits

RRM produces a network with optimal capacity, performance, and reliability while enabling you to avoid the cost of laborious historical data interpretation and individual lightweight access point reconfiguration. It also frees you from having to continually monitor the network for noise and interference problems, which can be transient and difficult to troubleshoot. Finally, RRM ensures that clients enjoy a seamless, trouble-free connection throughout the Cisco unified wireless network.

RRM uses separate monitoring and control for each deployed network: 802.11a and 802.11b/g. That is, the RRM algorithms run separately for each radio type (802.11a and 802.11b/g). RRM uses both measurements and algorithms. RRM measurements can be adjusted using monitor intervals, but they cannot be disabled. RRM algorithms, on the other hand, are enabled automatically but can be disabled by statically configuring channel and power assignment. The RRM algorithms run at a specified updated interval, which is 600 seconds by default.

# Overview of RF Groups

An RF group, also known as an RF domain, is a cluster of controllers that coordinates its RRM calculations on a per 802.11-network basis. An RF group exists for each 802.11 network type. Clustering controllers into RF groups enables the RRM algorithms to scale beyond a single controller.

Lightweight access points periodically send out neighbor messages over the air. Access points using the the same RF group name are able to validate messages from each other. When access points on different controllers hear validated neighbor messages at a signal strength of –80 dBm or stronger, the controllers dynamically form an RF group.

**Note** RF groups and mobility groups are similar in that they both define clusters of controllers, but they are different in terms of their use. These two concepts are often confused because the mobility group name and RF group name are configured to be the same in the Startup Wizard. Most of the time, all of the controllers in an RF group are also in the same mobility group and vice versa. However, an RF group facilitates scalable, system-wide dynamic RF management while a mobility group facilitates scalable, system-wide mobility and controller redundancy. Refer to the *Configuring Mobility Groups* chapter for more information on mobility groups.

Controller software release 4.2.99.0 or later supports up to 20 controllers and 1000 access points in an RF group. For example, a Cisco WiSM controller supports up to 150 access points, so you can have up to 6 WiSM controllers in an RF group (150 access points x 6 controllers = 900 access points, which is less than 1000). Similarly, a 4404 controller supports up to 100 access points, so you can have up to 10 4404 controllers in an RF group (100 x 10 = 1000). The 2100-series-based controllers support a maximum of 25 access points, so you can have up to 20 of these controllers in an RF group.

**Note** In controller software release 4.2.61.0 or earlier, RRM supports no more than five 4400-series-based controllers in an RF group.

# RF Group Leader

The members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).

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

In controller software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to controllers in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. That is, the worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio's channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors' neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings, if all the access point radios belong to the same RF group. This kind of domino effect in channel changes often results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and the fact that any potential channel plan changes are controlled by the RF circumstances of a single radio. In controller software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- **Multiple local searches**—The DCA search algorithm performs multiple local searches initiated by different radios within the same DCA run rather than performing a single global search 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 within the 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. Thus, 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. That is, the individual cost metrics of all 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 keep-alive 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 on page 11-10 for details.

## RF Group Name

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

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

# Configuring an RF Group

This section provides instructions for configuring RF groups through either the GUI or the CLI.

**Note** The RF group name is generally set at deployment time through the Startup Wizard. However, you can change it as necessary.

**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.

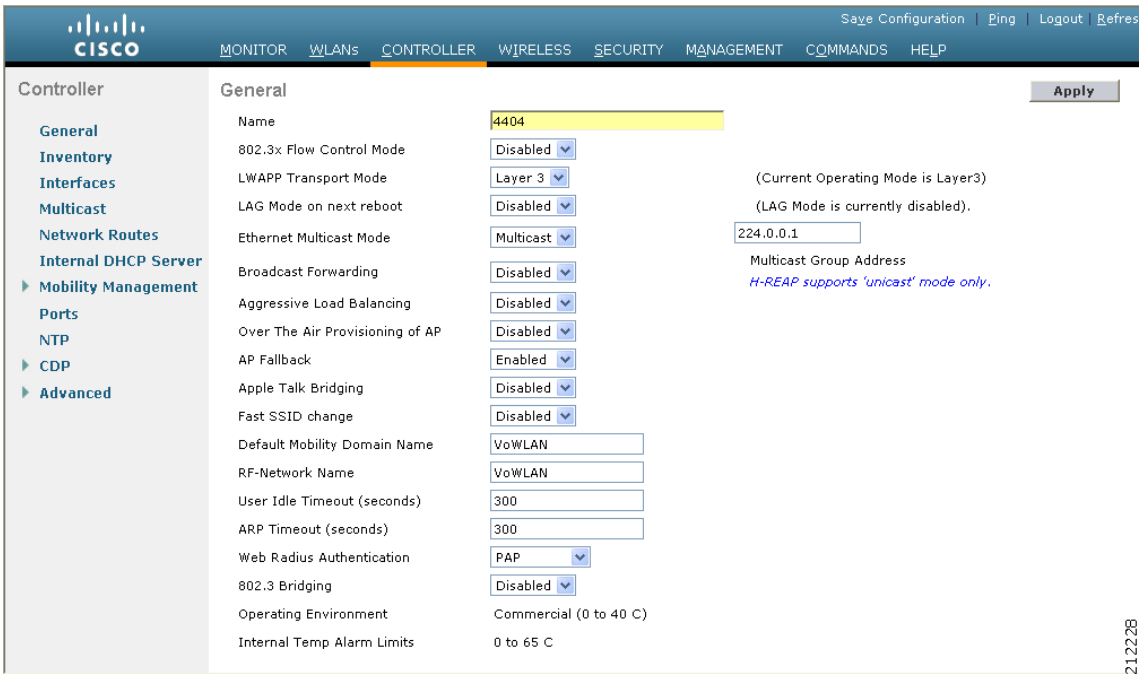
**Note** You can also configure RF groups using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.

## Using the GUI to Configure an RF Group

Follow these steps to create an RF group using the GUI.

**Step 1** Choose **Controller** > **General** to open the General page (see Figure 11-1).

*Figure 11-1 General Page*




**Step 2** Enter a name for the RF group in the RF-Network Name field. The name can contain up to 19 ASCII characters.

**Step 3** Click **Apply** to commit your changes.

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** Repeat this procedure for each controller that you want to include in the RF group.

# Using the CLI to Configure RF Groups

Follow these steps to configure an RF group using the CLI.

**Step 1** Enter **config network rf-network-name** *name* to create an RF group.

**Note** Enter up to 19 ASCII characters for the group name.

**Step 2** Enter **show network** to view the RF group.

**Step 3** Enter **save config** to save your settings.

**Step 4** Repeat this procedure for each controller that you want to include in the RF group.

# Viewing RF Group Status

This section provides instructions for viewing the status of the RF group through either the GUI or the CLI.

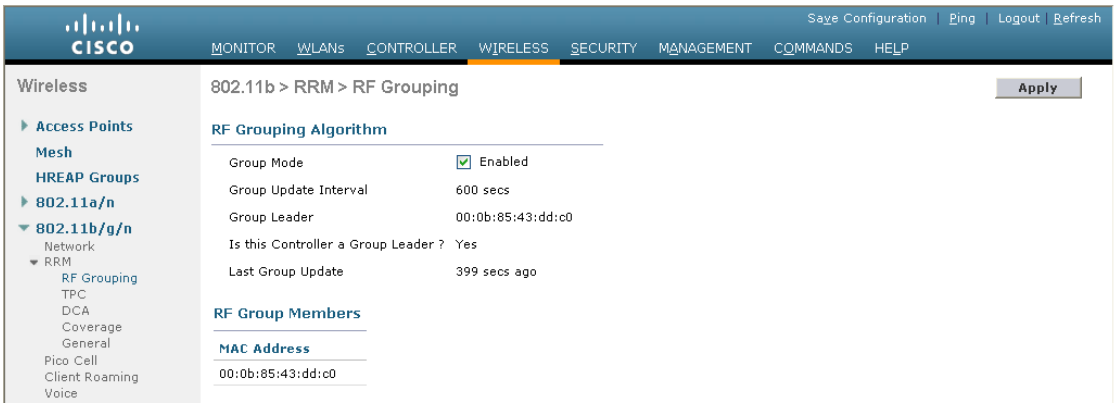
**Note** You can also view the status of RF groups using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.

## Using the GUI to View RF Group Status

Follow these steps to view the status of the RF group using the GUI.

**Step 1** Choose **Wireless > 802.11a/n** or **802.11b/g/n > RRM > RF Grouping** to open the 802.11a (or 802.11b/g) RRM > RF Grouping page (see Figure 11-2).

***Figure 11-2 802.11a > RRM > RF Grouping Page***




This page shows the details of the RF group, specifically how often the group information is updated (600 seconds by default), the MAC address of the RF group leader, whether this particular controller is the group leader, the last time the group information was updated, and the MAC addresses of all group members.

**Note** Automatic RF grouping, which is set through the **Group Mode** check box, is enabled by default. See the "Using the GUI to Configure RF Group Mode" section on page 11-11 for more information on this parameter.

**Step 2** If desired, repeat this procedure for the network type you did not select (802.11a or 802.11b/g).

## Using the CLI to View RF Group Status

Follow these steps to view the status of the RF group using the CLI.

**Step 1** Enter **show advanced 802.11a group** to see which controller is the RF group leader for the 802.11a RF network. Information similar to the following appears:

```
Radio RF Grouping
      802.11a Group Mode..............................  AUTO
      802.11a Group Update Interval...................  600 seconds
      802.11a Group Leader............................  00:16:9d:ca:d9:60
        802.11a Group Member..........................  00:16:9d:ca:d9:60
      802.11a Last Run................................  594 seconds ago
```

This text shows the details of the RF group, specifically whether automatic RF grouping is enabled for this controller, how often the group information is updated (600 seconds by default), the MAC address of the RF group leader, the MAC address of this particular controller, and the last time the group information was updated.

**Note** If the MAC addresses of the group leader and the group member are identical, this controller is currently the group leader.

**Step 2** Enter **show advanced 802.11b group** to see which controller is the RF group leader for the 802.11b/g RF network.

# Configuring RRM

The controller's preconfigured RRM settings are optimized for most deployments. However, you can modify the controller's RRM configuration parameters at any time through either the GUI or the CLI.

**Note** You can configure these parameters on controllers that are part of an RF group or on controllers that are not part of an RF group.

**Note** The RRM parameters should be set to the same values on every controller in an RF group. The RF group leader can change as a result of controller reboots or depending on which radios hear each other. If the RRM parameters are not identical for all RF group members, varying results can occur when the group leader changes.

## Using the GUI to Configure RRM

Using the controller GUI, you can configure the following RRM parameters: RF group mode, transmit power control, dynamic channel assignment, coverage hole detection, profile thresholds, monitoring channels, and monitor intervals. To configure these parameters, follow the instructions in the subsections below.

## Using the GUI to Configure RF Group Mode

Using the controller GUI, follow these steps to configure RF group mode.

**Step 1** Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **RRM** > **RF Grouping** to open the 802.11a (or 802.11b/g) RRM > RF Grouping page (see Figure 11-2).

**Step 2** Check the **Group Mode** check box to enable this controller to participate in an RF group, or uncheck it to disable this feature. If you enable this feature, the controller automatically forms an RF group with other controllers, and the group dynamically elects a leader to optimize RMM parameter settings for the the group. If you disable it, the controller does not participate in automatic RF grouping; instead it optimizes the access points connected directly to it. The default value is checked.

**Note** Cisco recommends that controllers participate in automatic RF grouping. Note that you can override RRM settings without disabling automatic RF group participation. See the "Overriding RRM" section on page 11-27 for instructions.

**Step 3** Click **Apply** to commit your changes.

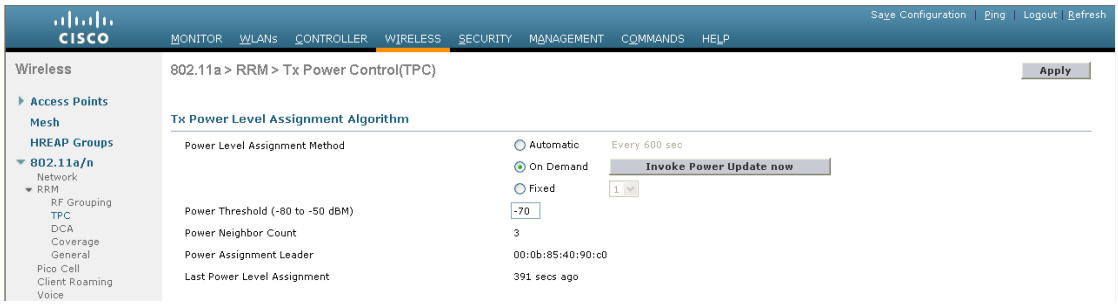
**Step 4** Click **Save Configuration** to save your changes.

## Using the GUI to Configure Transmit Power Control

Using the controller GUI, follow these steps to configure transmit power control settings.

**Step 1** Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **RRM** > **TPC** to open the 802.11a (or 802.11b/g) > RRM > Tx Power Control (TPC) page (see Figure 11-3).

*Figure 11-3 802.11a > RRM > Tx Power Control (TPC) Page*



**Step 2** Choose one of the following options from the Power Level Assignment Method drop-down box to specify the controller's dynamic power assignment mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
- **On Demand**—Causes the controller to periodically evaluate the transmit power for all joined access points. However, the controller updates the power, if necessary, only when you click **Invoke Power Update Now**.

**Note** The controller does not evaluate and update the transmit power immediately after you click **Invoke Power Update Now**. It waits for the next 600-second interval. This value is not configurable.

- **Fixed**—Prevents the controller from evaluating and, if necessary, updating the transmit power for joined access points. The power level is set to the fixed value chosen from the drop-down box.

**Note** The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. See Step 7 on page 11-31 for information on available transmit power levels.

**Note** For optimal performance, Cisco recommends that you use the Automatic setting. Refer to the "Disabling Dynamic Channel and Power Assignment Globally for a Controller" section on page 11-35 for instructions if you ever need to disable the controller's dynamic channel and power settings.

**Step 3** 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 is –70 dBm but can be changed when access points are transmitting at higher (or lower) than desired power levels.

The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

This page also shows the following non-configurable transmit power level parameter settings:

- **Power Neighbor Count**—The minimum number of neighbors an access point must have for the transmit power control algorithm to run.
- **Power Assignment Leader**—The MAC address of the RF group leader, which is responsible for power level assignment.
- **Last Power Level Assignment**—The last time RRM evaluated the current transmit power level assignments.

**Step 4** Click **Apply** to commit your changes.

**Step 5** Click **Save Configuration** to save your changes.

### Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm has undergone a major rework in this release and it should do an adequate job of balancing 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 only apply to access points attached to a controller from which they are configured; it is not a global RRM command. Note that the default settings essentially disable this feature, and you should use care when overriding TPC recommendations.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment fields, enter the maximum and minimum transmit power used by RRM on the Tx Power Controle 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 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, then no access point would transmit above 11 dBm, unless the access point is configured manually.

## Using the GUI to Configure Dynamic Channel Assignment

Using the controller GUI, follow these steps to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning. This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

**Note** If a WLAN is configured to an 802.11g only radio policy and a LAP is configured to channel 14, then the WLAN clients try to associate with the LAP, which does not work as expected because of the 802.11g only policy. The workaround to the problem is one of the following:
- Disable channel 14 manually when 802.11g only policy is configured in WLANs.
- Do not select 802.11g only policy when channel 14 is configured to a LAP.

**Step 1** To disable the 802.11a or 802.11b/g network, follow these steps:

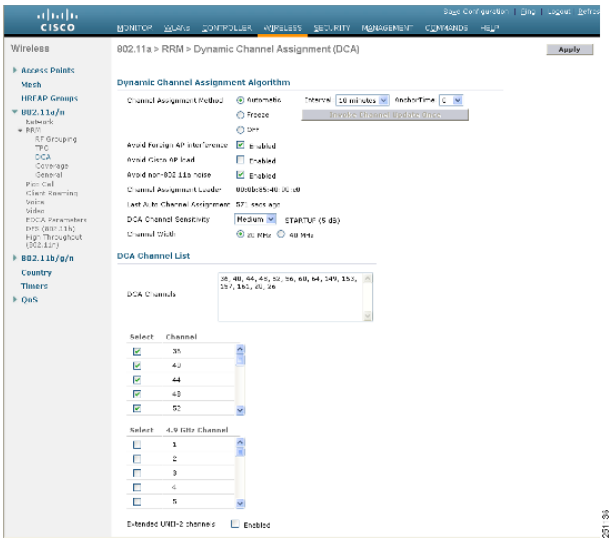
a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 2** Choose **Wireless > 802.11a/n** or **802.11b/g/n > RRM > DCA** to open the 802.11a (or 802.11b/g) > RRM > Dynamic Channel Assignment (DCA) page (see Figure 11-4).

*Figure 11-4 802.11a > RRM > Dynamic Channel Assignment (DCA) Page*




**Step 3** Choose one of the following options from the Channel Assignment Method drop-down box to specify the controller's DCA mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.
- **Freeze**—Causes the controller to evaluate and update the channel assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**.

  **Note** The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all access point 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.

**Note** For optimal performance, Cisco recommends that you use the Automatic setting. Refer to the "Disabling Dynamic Channel and Power Assignment Globally for a Controller" section on page 11-35 for instructions if you ever need to disable the controller's dynamic channel and power settings.

**Step 4** From the Interval drop-down box, choose one of the following options to specify how often the DCA algorithm is allowed to run: 10 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 6 hours, 8 hours, 12 hours, or 24 hours. The default value is 10 minutes.

**Note** If your controller supports only OfficeExtend access points, Cisco recommends that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

**Step 5** From the AnchorTime drop-down box, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

**Step 6** Check the **Avoid Foreign AP Interference** check box to cause the controller's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is checked.

**Step 7** Check the **Avoid Cisco AP Load** check box to cause the controller's RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels, or uncheck it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is unchecked.

**Step 8** Check the **Avoid Non-802.11a (802.11b) Noise** check box to cause the controller's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may have access points avoid channels with significant interference from non-access point sources, such as microwave ovens. The default value is checked.

**Step 9** From the DCA Channel Sensitivity drop-down box, 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.
- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.
- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is Medium. The DCA sensitivity thresholds vary by radio band, as noted in Table 11-1.

*Table 11-1 DCA Sensitivity Thresholds*

| Option | 2.4-GHz DCA Sensitivity Threshold | 5-GHz DCA Sensitivity Threshold |
|---|---|---|
| High | 5 dB | 5 dB |
| Medium | 10 dB | 15 dB |
| Low | 20 dB | 20 dB |

**Step 10** For 802.11a/n networks only, choose one of the following Channel Width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)
- **40 MHz**—The 40-MHz channel bandwidth

**Note** If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List in Step 11 (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

**Note** If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points. Refer to the "Using the GUI to Statically Assign Channel and Transmit Power Settings" section on page 11-28 for configuration instructions.

**Note** To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode on the 802.11a/n Cisco APs > Configure page. If you ever then change the static RF channel assignment method to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

This page also shows the following non-configurable channel parameter settings:

- **Channel Assignment Leader**—The MAC address of the RF group leader, which is responsible for channel assignment.
- **Last Auto Channel Assignment**—The last time RRM evaluated the current channel assignments.

**Step 11** In the DCA Channel List section, the DCA Channels field shows the channels that are currently selected. To choose a channel, check its check box in the Select column. To exclude a channel, uncheck its check box.

**Range:**
802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165, 190, 196
802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

**Default:**
802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161
802.11b/g—1, 6, 11

**Note** These extended UNII-2 channels in the 802.11a band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, check the **Extended UNII-2 Channels** check box.

**Step 12** If you are using Cisco Aironet 1520 series mesh access points in your network, you need to set the 4.9-GHz channels in the 802.11a band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, check its check box in the Select column. To exclude a channel, uncheck its check box.

**Range:**
802.11a—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26

**Default:**
802.11a—20, 26

**Step 13** Click **Apply** to commit your changes.

**Step 14** To re-enable the 802.11a or 802.11b/g network, follow these steps:

a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 15** Click **Save Configuration** to save your changes.

**Note** To see why the DCA algorithm changed channels, choose **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

## Using the GUI to Configure Coverage Hole Detection

Using the controller GUI, follow these steps to enable coverage hole detection.

**Note** In controller software release 5.2 or later, you can disable coverage hole detection on a per-WLAN basis. See the "Disabling Coverage Hole Detection per WLAN" section on page 6-65 for more information.

**Step 1** To disable the 802.11a or 802.11b/g network, follow these steps:

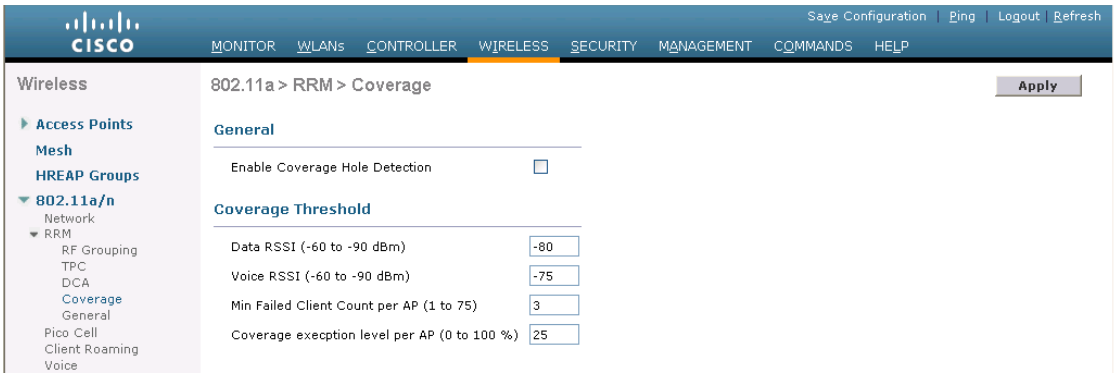
a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 2** Choose **Wireless > 802.11a/n** or **802.11b/g/n > RRM > Coverage** to open the 802.11a (or 802.11b/g) > RRM > Coverage page (see Figure 11-5).

*Figure 11-5 802.11a > RRM > Coverage Page*




**Step 3** Check the **Enable Coverage Hole Detection** check box to enable coverage hole detection, or uncheck it to disable this feature. If you enable coverage hole detection, the controller automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is checked.

**Step 4** In the Data RSSI field, enter the minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

**Step 5** In the Voice RSSI field, enter the minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –75 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

**Step 6** In the Min Failed Client Count per AP field, enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

**Step 7** In the Coverage Exception Level per AP field, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

**Note** If both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the controller CLI; see page 11-24) for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP fields over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

**Step 8** Click **Apply** to commit your changes.

**Step 9** To re-enable the 802.11a or 802.11b/g network, follow these steps:

a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

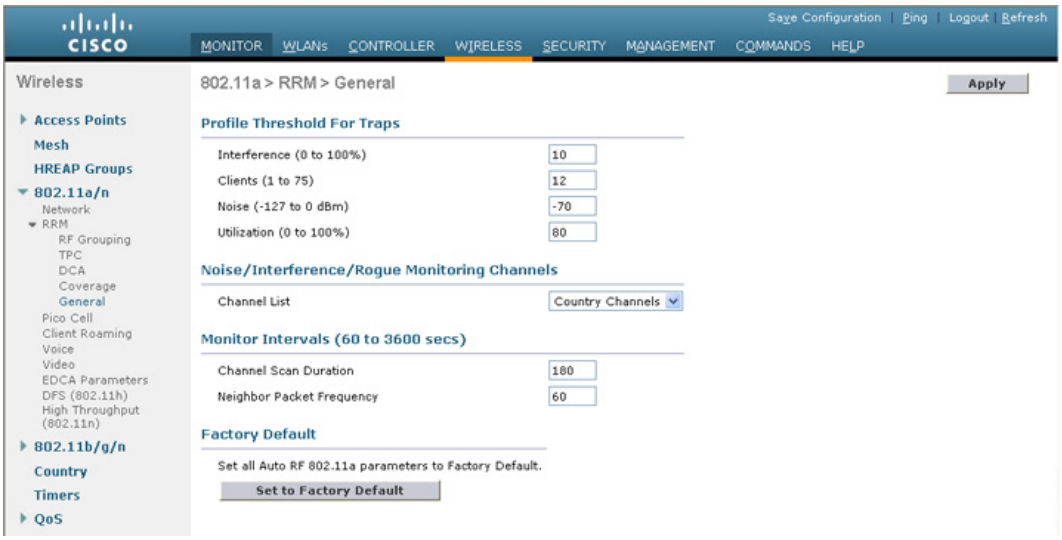
**Step 10** Click **Save Configuration** to save your changes.

## Using the GUI to Configure RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals

Using the controller GUI, follow these steps to configure RRM profile thresholds, monitoring channels, and monitor intervals.

**Step 1** Choose **Wireless > 802.11a/n** or **802.11b/g/n > RRM > General** to open the 802.11a (or 802.11b/g) > RRM > General page (see Figure 11-6).

*Figure 11-6 802.11a > RRM > General Page*




**Step 2** To configure profile thresholds used for alarming, follow these steps.

**Note** The profile thresholds have no bearing on the functionality of the RRM algorithms. Lightweight access points send an SNMP trap (or an alert) to the controller when the values set for these threshold parameters are exceeded.

a. In the Interference field, enter the percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. The valid range is 0 to 100%, and the default value is 10%.

b. In the Clients field, enter the number of clients on a single access point. The valid range is 1 to 75, and the default value is 12.

c. In the Noise field, enter the level of noise (non-802.11 traffic) on a single access point. The valid range is –127 to 0 dBm, and the default value is –70 dBm.

d. In the Utilization field, enter the percentage of RF bandwidth being used by a single access point. The valid range is 0 to 100%, and the default value is 80%.

**Step 3** From the Channel List drop-down box, choose one of the following options to specify the set of channels that the access point uses for RRM scanning:

- **All Channels**—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
- **Country Channels**—RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
- **DCA Channels**—RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired. To do so, follow the instructions in the "Using the GUI to Configure Dynamic Channel Assignment" section on page 11-13.

**Step 4** To configure monitor intervals, follow these steps:

a. In the Channel Scan Duration field, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at the Channel Scan Duration interval. The time spent listening on each channel is determined by the non-configurable 50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms is spent listening on each scanned channel (180/11 = ~16 seconds). The Channel Scan Duration parameter determines the interval at which the scanning occurs.The valid range is 60 to 3600 seconds, and the default value is 180 seconds for the 802.11a radios and the 802.11b/g radios.

**Note** If your controller supports only OfficeExtend access points, Cisco recommends that you set the channel scan duration to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

b. In the Neighbor Packet Frequency field, enter (in seconds) how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default value is 60 seconds.

**Note** If your controller supports only OfficeExtend access points, Cisco recommends that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

**Note** In controller software release 4.1.185.0 or later, if the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the controller deletes that neighbor from the neighbor list. In controller software releases prior to 4.1.185.0, the controller waits only 20 minutes before deleting an unresponsive neighbor radio from the neighbor list.

**Step 5** Click **Apply** to commit your changes.

**Step 6** Click **Save Configuration** to save your changes.

**Note** Click **Set to Factory Default** if you ever want to return all of the controller's RRM parameters to their factory default values.

# Using the CLI to Configure RRM

Using the controller CLI, follow these steps to configure RRM.

**Step 1** Enter this command to disable the 802.11a or 802.11b/g network:

**config {802.11a | 802.11b} disable network**

**Step 2** Perform one of the following to configure transmit power control:

- To have RRM automatically set the transmit power for all 802.11a or 802.11b/g radios at periodic intervals, enter this command:

  **config {802.11a | 802.11b} txPower global auto**

- To have RRM automatically reset the transmit power for all 802.11a or 802.11b/g radios one time, enter this command:

  **config {802.11a | 802.11b} txPower global once**

- To configure the transmit power range that overrides the Transmit Power Control algorithm, use this command to enter the maximum and minimum trnasmit power used by RRM:

  **config {802.11a | 802.11b} txPower global {max | min}** *txpower*

  where *txpower* is a value 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 to exceed this transmit power (whether the maximum is set at RRM startup, or by Coverage Hole Detection). For example, if you configure a maximum transmit power of 11 dBm, then no access opint would transmit above 11 dBm, unless the access point is configured manually.

- To manually change the default transmit power setting of –70 dBm, enter this command:

  **config advanced {802.11a | 802.11b} tx-power-control-thresh** *threshold*

  where *threshold* is a value from –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect.

  In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients may have difficulty processing a large number of BSSIDs or a high beacon rate and may exhibit problematic behavior with the default threshold.

**Step 3** Perform one of the following to configure dynamic channel assignment (DCA):

- To have RRM automatically configure all 802.11a or 802.11b/g channels based on availability and interference, enter this command:

  **config {802.11a | 802.11b} channel global auto**

- To have RRM automatically reconfigure all 802.11a or 802.11b/g channels one time based on availability and interference, enter this command:

  **config {802.11a | 802.11b} channel global once**

- To disable RRM and set all channels to their default values, enter this command:

  **config {802.11a | 802.11b} channel global off**

- To specify the channel set used for DCA, enter this command:

  **config advanced {802.11a | 802.11b} channel {add | delete}** *channel_number*

  You can enter only one channel number per command. This command is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

**Step 4** Use these commands to configure additional DCA parameters:

- **config advanced {802.11a | 802.11b} channel dca anchor-time** *value*—Specifies the time of day when the DCA algorithm is to start. *Valu*e is a number between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.
- **config advanced {802.11a | 802.11b} channel dca interval** *value*—Specifies how often the DCA algorithm is allowed to run. *Valu*e is one of the following: 1, 2, 3, 4, 6, 8, 12, or 24 hours or 0, which is the default value of 10 minutes (or 600 seconds).

  **Note** If your controller supports only OfficeExtend access points, Cisco recommends that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

- **config advanced {802.11a | 802.11b} channel dca sensitivity {low | medium | high}**—Specifies how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channel.
  - **low** means that the DCA algorithm is not particularly sensitive to environmental changes.
  - **medium** means that the DCA algorithm is moderately sensitive to environmental changes.
  - **high** means that the DCA algorithm is highly sensitive to environmental changes.

  The DCA sensitivity thresholds vary by radio band, as noted in Table 11-2.

***Table 11-2 DCA Sensitivity Thresholds***

| Option | 2.4-GHz DCA Sensitivity Threshold | 5-GHz DCA Sensitivity Threshold |
|---|---|---|
| High | 5 dB | 5 dB |
| Medium | 15 dB | 20 dB |
| Low | 30 dB | 35 dB |

- **config advanced 802.11a channel dca chan-width-11n** {**20** | **40**}—Configures the DCA channel width for all 802.11n radios in the 5-GHz band, where
  - **20** sets the channel width for 802.11n radios to 20 MHz. This is the default value.
  - **40** sets the channel width for 802.11n radios to 40 MHz.

**Note** If you choose 40, be sure to set at least two adjacent channels in the **config advanced 802.11a channel** {**add** | **delete**} *channel_number* command in Step 3 (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for 40-MHz channel width.

**Note** If you choose 40, you can also configure the primary and extension channels used by individual access points. Refer to the "Using the CLI to Statically Assign Channel and Transmit Power Settings" section on page 11-32 for configuration instructions.

**Note** To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode using the **config 802.11a chan_width** *Cisco_AP* {**20** | **40**} command. If you ever then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

- **config advanced** {**802.11a** | **802.11b**} **channel foreign** {**enable** | **disable**}—Enables or disables foreign access point interference avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel load** {**enable** | **disable**}—Enables or disables load avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel noise** {**enable** | **disable**}—Enables or disables noise avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel update**—Initiates an update of the channel selection for every Cisco access point.

**Step 5** Use these commands to configure coverage hole detection:

**Note** In controller software release 5.2 or later, you can disable coverage hole detection on a per-WLAN basis. See the "Disabling Coverage Hole Detection per WLAN" section on page 6-65 for more information.

- **config advanced** {**802.11a** | **802.11b**} **coverage** {**enable** | **disable**}—Enables or disables coverage hole detection. If you enable coverage hole detection, the controller automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is enabled.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*—Specifies the minimum receive signal strength indication (RSSI) value for packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value below the value you enter here, a potential coverage hole has been detected. The valid range is –90 to –60

dBm, and the default value is –80 dBm for data packets and –75 dBm for voice packets. The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

- **config advanced** {**802.11a** | **802.11b**} **coverage level global** *clients*—Specifies the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.
- **config advanced** {**802.11a** | **802.11b**} **coverage exception global** *percent*—Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **packet-count** *packets*—Specifies the minimum failure count threshold for uplink data or voice packets. The valid range is 1 to 255 packets, and the default value is 10 packets.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **fail-rate** *percent*—Specifies the failure rate threshold for uplink data or voice packets. The valid range is 1 to 100%, and the default value is 20%.

**Note** If both the number and percentage of failed packets exceed the values entered in the **packet-count** and **fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **coverage level global** and **coverage exception global** commands over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

**Step 6** Enter this command to enable the 802.11a or 802.11b/g network:

**config** {**802.11a** | **802.11b**} **enable network**

**Note** To enable the 802.11g network, enter **config 802.11b 11gSupport enable** after the **config 802.11b enable network** command.

**Step 7** Enter this command to save your settings:

**save config**

# Using the CLI to View RRM Settings

Use these commands to view 802.11a and 802.11b/g RRM settings:

**show advanced** {**802.11a** | **802.11b**} *?*

where *?* is one of the following:

- **ccx** {**global** | *Cisco_AP*}—Shows the CCX RRM configuration.

```
802.11a Client Beacon Measurements:
    disabled
```

- **channel**—Shows the channel assignment configuration and statistics.

```
Automatic Channel Assignment
  Channel Assignment Mode....................... ONCE
  Channel Update Interval....................... 600 seconds
  Anchor time (Hour of the day)................. 20
  Channel Update Count.......................... 0
  Channel Update Contribution................... S.IU
  Channel Assignment Leader..................... 00:0b:85:40:90:c0
  Last Run...................................... 532 seconds ago
  DCA Sensitivity Level......................... MEDIUM (20 dB)
  DCA 802.11n Channel Width..................... 40 MHz
  Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Auto-RF Allowed Channel List.................. 36,40
  Auto-RF Unused Channel List................... 44,48,52,56,60,64,100,104,
    ..................................... 108,112,116,132,136,140,149,
    ..................................... 153,157,161,165,190,196
  DCA Outdoor AP option...................... Disabled
```

- **coverage**—Shows the coverage hole detection configuration and statistics.

```
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode........... Enabled
  802.11a Coverage Voice Packet Count............ 10 packets
  802.11a Coverage Voice Packet Percentage....... 20%
  802.11a Coverage Voice RSSI Threshold.......... -75 dBm
  802.11a Coverage Data Packet Count............. 10 packets
  802.11a Coverage Data Packet Percentage........ 20%
  802.11a Coverage Data RSSI Threshold........... -80 dBm
  802.11a Global coverage exception level........ 25%
  802.11a Global client minimum exception lev. 3 clients
```

- **logging**—Shows the RF event and performance logging.

```
RF Event and Performance Logging
  Channel Update Logging......................... Off
  Coverage Profile Logging....................... Off
  Foreign Profile Logging........................ Off
  Load Profile Logging........................... Off
  Noise Profile Logging.......................... Off
  Performance Profile Logging.................... Off
  TxPower Update Logging..................... Off
```

- **monitor**—Shows the Cisco radio monitoring.

```
Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Channels....................... Country channels
  802.11a AP Coverage Interval................... 180 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Noise Interval...................... 180 seconds
  802.11a AP Signal Strength Interval......... 60 seconds
```

- **profile** {**global** | *Cisco_AP*}—Shows the access point performance profiles.

```
Default 802.11a AP performance profiles
  802.11a Global Interference threshold.......... 10%
  802.11a Global noise threshold................. -70 dBm
```

```
  802.11a Global RF utilization threshold........ 80%
  802.11a Global throughput threshold............ 1000000 bps
  802.11a Global clients threshold............ 12 clients
```

- **receiver**—Shows the 802.11a or 802.11b/g receiver configuration and statistics.

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 15
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 2
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Enabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Enabled
 TxStomp  : Wrong BSSID Data Only Status......... Enabled
 RxAbort  : Raw Power Drop Status................ Disabled
 RxAbort  : Raw Power Drop Threshold............. 10
 RxAbort  : Low RSSI Status...................... Disabled
 RxAbort  : Low RSSI Threshold................... 0
 RxAbort  : Wrong BSSID Status................... Disabled
 RxAbort  : Wrong BSSID Data Only Status......... Disabled
 ---------------------------------------....
 pico-cell-V2 parameters in dbm units:...........

 RxSensitivity: Min,Max,Current RxSense Thres.... 0,0,0
 CCA Threshold: Min,Max,Current Clear Channel.... 0,0,0
Tx Pwr: Min,Max,Current Transmit Power for A.... 0,0,0
 ---------------------------------------....
```

- **summary**—Shows the configuration and statistics of the 802.11a or 802.11b/g access points.

```
AP Name   MAC Address        Admin State  Operation State Channel TxPower
-------- ----------------- ------------ --------------- -------- -------
AP1140   00:22:90:96:5b:d0    ENABLED         DOWN        64*     1(*)
AP1240   00:21:1b:ea:36:60    ENABLED         DOWN       161*     1(*)
AP1130   00:1f:ca:cf:b6:60    ENABLED      REGISTERED    48*     1(*)
```

- **txpower**—Shows the transmit power assignment configuration and statistics.

```
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 600 seconds
  Transmit Power Update Count.................... 0
  Transmit Power Threshold....................... -70 dBm
  Transmit Power Neighbor Count.................. 3 APs
  Min Transmit Power............................. -100 dBm
  Max Transmit Power............................. 100 dBm
  Transmit Power Update Contribution............. SNI.
  Transmit Power Assignment Leader............... 00:0b:85:40:90:c0
  Last Run....................................... 354 seconds ago
```

# Using the CLI to Debug RRM Issues

Use these commands to troubleshoot and verify RRM behavior:

**debug airewave-director** *?*

where *?* is one of the following:

- **all**—Enables debugging for all RRM logs.
- **channel**—Enables debugging for the RRM channel assignment protocol.

- **detail**—Enables debugging for RRM detail logs.
- **error**—Enables debugging for RRM error logs.
- **group**—Enables debugging for the RRM grouping protocol.
- **manager**—Enables debugging for the RRM manager.
- **message**—Enables debugging for RRM messages.
- **packet**—Enables debugging for RRM packets.
- **power**—Enables debugging for the RRM power assignment protocol as well as coverage hole detection.
- **profile**—Enables debugging for RRM profile events.
- **radar**—Enables debugging for the RRM radar detection/avoidance protocol.
- **rf-change**—Enables debugging for RRM RF changes.

# Overriding RRM

In some deployments, it is desirable to statically assign channel and transmit power settings to the access points instead of relying on the RRM algorithms provided by Cisco. Typically, this is true in challenging RF environments and non-standard deployments but not the more typical carpeted offices.

**Note** If you choose to statically assign channels and power levels to your access points and/or to disable dynamic channel and power assignment, you should still use automatic RF grouping to avoid spurious rogue device events.

You can disable dynamic channel and power assignment globally for a controller, or you can leave dynamic channel and power assignment enabled and statically configure specific access point radios with a channel and power setting. Follow the instructions in one of the following sections:

- Statically Assigning Channel and Transmit Power Settings to Access Point Radios, page 11-28
- Disabling Dynamic Channel and Power Assignment Globally for a Controller, page 11-35

**Note** While you can specify a global default transmit power parameter for each network type that applies to all the access point radios on a controller, you must set the channel for each access point radio when you disable dynamic channel assignment. You may also want to set the transmit power for each access point instead of leaving the global transmit power in effect.

# Statically Assigning Channel and Transmit Power Settings to Access Point Radios

This section provides instructions for statically assigning channel and power settings using the GUI or CLI.

**Note** Cisco recommends that you assign different nonoverlapping channels to access points that are within close proximity to each other. The nonoverlapping channels in the U.S. are 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, and 161 in an 802.11a network and 1, 6, and 11 in an 802.11b/g network.

**Note** Cisco recommends that you do not assign all access points that are within close proximity to each other to the maximum power level.

## Using the GUI to Statically Assign Channel and Transmit Power Settings

Follow these steps to statically assign channel and/or power settings on a per access point radio basis using the GUI.

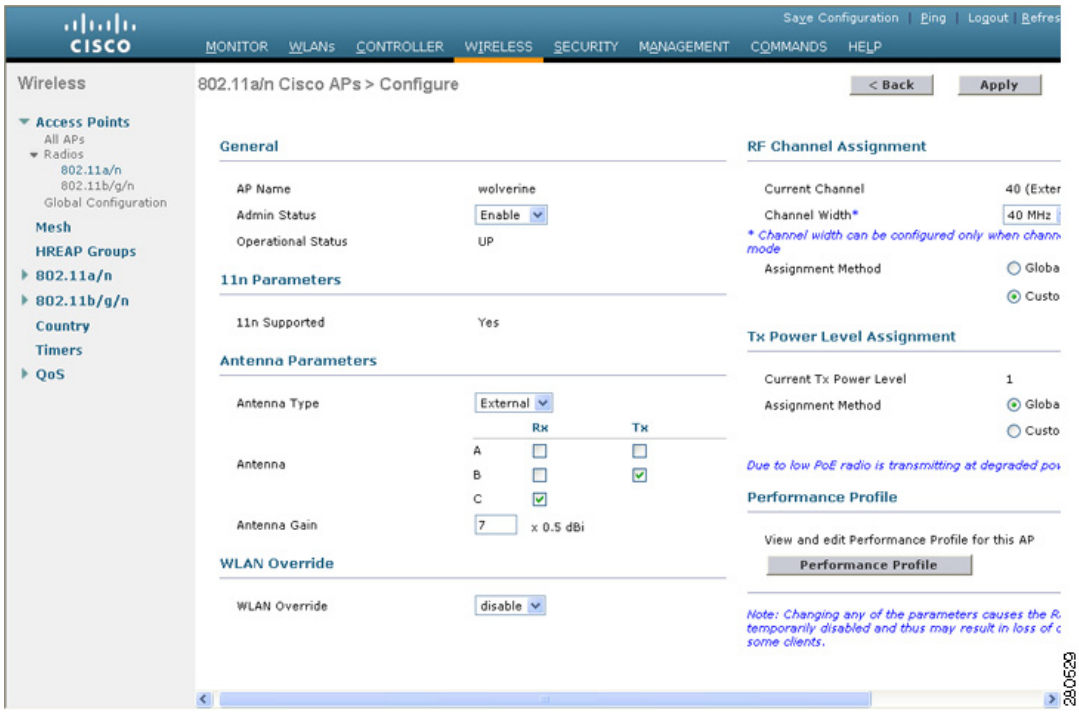
**Step 1** Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n** or **802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page (see Figure 11-7).

***Figure 11-7 802.11a/n Radios Page***


This page shows all the 802.11a/n or 802.11b/g/n access point radios that are joined to the controller and their current settings. The Channel field shows both the primary and extension channels and uses an asterisk to indicate if they are globally assigned.

**Step 2** Hover your cursor over the blue drop-down arrow for the access point for which you want to modify the radio configuration and choose **Configure**. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears (see Figure 11-8).

*Figure 11-8 802.11a/n Cisco APs > Configure Page*




**Step 3** To be able to assign primary and extension channels to the access point radio, choose **Custom** for the Assignment Method under RF Channel Assignment.

**Step 4** Choose one of the following options from the Channel Width drop-down box:

- **20 MHz**—Allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.
- **40 MHz**—Allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose in Step 6 as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the controller would use channel 48 as the extension channel. Conversely, if you choose a primary channel of 48, the controller would use channel 44 as the extension channel.

**Note** Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

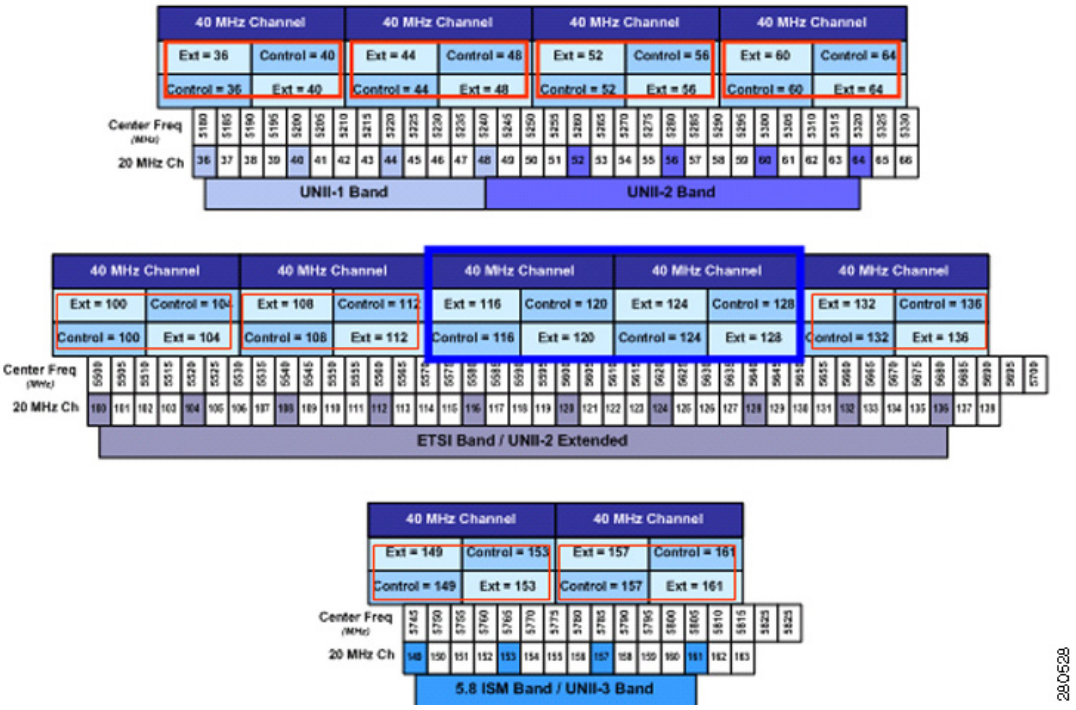
**Note** The Channel Width parameter can be configured for 802.11a/n radios only if the RF channel assignment method is in custom mode and for 802.11b/g/n radios only if both the RF channel assignment method and the Tx power level assignment method are in custom mode.

**Note** Statically configuring an access point's radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting on the 802.11a > RRM > Dynamic Channel Assignment (DCA) page. If you ever change the static RF channel assignment method back to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

Figure 11-9 illustrates channel bonding in the 5-GHz band. Low channels are preferred.

**Note** Channels 116, 120, 124, and 128 are not available in the U.S. and Canada for 40-MHz channel bonding.

***Figure 11-9 Channel Bonding in the 5-GHz Band***




**Step 5** Follow these steps to configure the antenna parameters for this radio:

**a.** From the Antenna Type drop-down box, choose **Internal** or **External** to specify the type of antennas used with the access point radio.

**b.** Check and uncheck the check boxes in the Antenna field to enable and disable the use of specific antennas for this access point, where A, B, and C are specific antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from antenna ports A and B and receptions from antenna port C, you would check the following check boxes: Tx: A and B and Rx: C.

c. In the Antenna Gain field, enter a number to specify an external antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

   If you have a high-gain antenna, enter a value that is twice the actual dBi value (refer to the *Cisco Aironet Antenna Reference Guide* for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The controller reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations.

d. Choose one of the following options from the Diversity drop-down box:

   - **Enabled**—Enables the antenna connectors on both sides of the access point. This is the default value.
   - **Side A** or **Right**—Enables the antenna connector on the right side of the access point.
   - **Side B** or **Left**—Enables the antenna connector on the left side of the access point.

**Step 6** To assign an RF channel to the access point radio, choose **Custom** for the Assignment Method under RF Channel Assignment and choose a channel from the drop-down box.

The channel you choose is the primary channel (for example, channel 36), which is used for communication by legacy 802.11a radios and 802.11n 20-MHz radios. 802.11n 40-MHz radios use this channel as the primary channel but also use an additional bonded extension channel for faster throughput, if you chose 40 MHz for the channel width in Step 4.

**Note** The Current Channel field shows the current primary channel. If you chose 40 MHz for the channel width in Step 4, the extension channel appears in parentheses after the primary channel.

**Note** Changing the operating channel causes the access point radio to reset.

**Step 7** To assign a transmit power level to the access point radio, choose **Custom** for the Assignment Method under Tx Power Level Assignment and choose a transmit power level from the drop-down box.

The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

**Note** Refer to the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, refer to the data sheet for your access point for the number of power levels supported.

**Note** If the access point is not operating at full power, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section. Refer to the "Configuring Power over Ethernet" section on page 7-98 for more information on PoE power levels.

**Step 8** To enable this configuration for the access point, choose **Enable** from the Admin Status drop-down box.

**Step 9** Click **Apply** to commit your changes.

**Step 10** To have the controller send the access point radio admin state immediately to WCS, follow these steps:

a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 11** Click **Save Configuration** to save your changes.

**Step 12** Repeat this procedure for each access point radio for which you want to assign a static channel and power level.

## Using the CLI to Statically Assign Channel and Transmit Power Settings

Follow these steps to statically assign channel and/or power settings on a per access point radio basis using the CLI.

**Step 1** To disable the radio of a particular access point on the 802.11a or 802.11b/g network, enter this command:

**config** {**802.11a** | **802.11b**} **disable** *Cisco_AP*

**Step 2** To configure the channel width for a particular access point, enter this command:

**config** {**802.11a** | **802.11b**} **chan_width** *Cisco_AP* {**20** | **40**}

where

- **20** allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.
- **40** allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose in Step 5 as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the controller would use channel 48 as the extension channel. Conversely, if you choose a primary channel of 48, the controller would use channel 44 as the extension channel.

**Note** This parameter can be configured only if the primary channel is statically assigned.

**Note** Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

**Note** Statically configuring an access point's radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting (configured using the **config advanced 802.11a channel dca chan-width-11n** {**20** | **40**} command). If you ever change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

Figure 11-9 on page 11-30 shows channel bonding in the 5-GHz band. Low channels are preferred.

**Note** Channels 116, 120, 124, and 128 are not available in the U.S. and Canada for 40-MHz channel bonding.

**Step 3** To enable or disable the use of specific antennas for a particular access point, enter this command:

**config** {**802.11a** | **802.11b**} **11nsupport antenna** {**tx** | **rx**} *Cisco_AP* {**A** | **B** | **C**} {**enable** | **disable**}

where A, B, and C are antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from the antenna in access point AP1's antenna port C on the 802.11a network, you would enter the following command:

**config 802.11a 11nsupport antenna tx AP1 C enable**

**Step 4** To specify the external antenna gain, which is a measure of an external antenna's ability to direct or focus radio energy over a region of space, enter this command:

**config** {**802.11a** | **802.11b**} **antenna extAntGain** *antenna_gain Cisco_AP*

High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (refer to the *Cisco Aironet Antenna Reference Guide* for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The controller reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations.

**Step 5** To specify the channel that a particular access point is to use, enter this command:

**config** {**802.11a** | **802.11b**} **channel ap** *Cisco_AP channel*

Example: To configure 802.11a channel 36 as the default channel on AP1, enter this command: **config 802.11a channel ap AP1 36**.

The channel you choose is the primary channel (for example, channel 36), which is used for communication by legacy 802.11a radios and 802.11n 20-MHz radios. 802.11n 40-MHz radios use this channel as the primary channel but also use an additional bonded extension channel for faster throughput, if you chose 40 for the channel width in Step 2.

**Note** Changing the operating channel causes the access point radio to reset.

**Step 6** To specify the transmit power level that a particular access point is to use, enter this command:

**config** {**802.11a** | **802.11b**} **txPower ap** *Cisco_AP power_level*

Example: To set the transmit power for 802.11a AP1 to power level 2, enter this command: **config 802.11a txPower ap AP1 2**.

The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

**Note** Refer to the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, refer to the data sheet for your access point for the number of power levels supported.

**Step 7** To save your settings, enter this command:

**save config**

**Step 8** Repeat Step 2 through Step 7 for each access point radio for which you want to assign a static channel and power level.

**Step 9** To re-enable the access point radio, enter this command:

**config {802.11a | 802.11b} enable** *Cisco_AP*

**Step 10** To have the controller send the access point radio admin state immediately to WCS, enter this command:

**config {802.11a | 802.11b} enable network**

**Step 11** To save your settings, enter this command:

**save config**

**Step 12** To see the configuration of a particular access point, enter this command:

**show ap config {802.11a | 802.11b}** *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 7
Cisco AP Name.................................... AP1
...
Tx Power
Num Of Supported Power Levels ............. 8
      Tx Power Level 1 ........................... 20 dBm
      Tx Power Level 2 ........................... 17 dBm
      Tx Power Level 3 ........................... 14 dBm
      Tx Power Level 4 ........................... 11 dBm
      Tx Power Level 5 ........................... 8 dBm
      Tx Power Level 6 ........................... 5 dBm
      Tx Power Level 7 ........................... 2 dBm
      Tx Power Level 8 ........................... -1 dBm
      Tx Power Configuration ..................... CUSTOMIZED
      Current Tx Power Level ..................... 1

Phy OFDM parameters
      Configuration .............................. CUSTOMIZED
      Current Channel ............................ 36
      Extension Channel .......................... 40
      Channel Width.............................. 40 Mhz
      Allowed Channel List....................... 36,44,52,60,100,108,116,132,
        ......................................... 149,157
      TI Threshold ............................... -50
      Antenna Type............................... EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBi units).... 7
      Diversity.................................. DIVERSITY_ENABLED
```

```
802.11n Antennas
        Tx
         A..................................... ENABLED
         B..................................... ENABLED
        Rx
         A..................................... DISABLED
         B..................................... DISABLED
         C..................................... ENABLED
```

# Disabling Dynamic Channel and Power Assignment Globally for a Controller

This section provides instructions for disabling dynamic channel and power assignment using the GUI or CLI.

## Using the GUI to Disable Dynamic Channel and Power Assignment

Follow these steps to configure disable dynamic channel and power assignment using the GUI.

**Step 1** Choose **Wireless > 802.11a/n** or **802.11b/g/n > RRM > Auto RF** to open the 802.11a (or 802.11b/g) Global Parameters > Auto RF page (see Figure 11-2).

**Step 2** To disable dynamic channel assignment, choose **OFF** under RF Channel Assignment.

**Step 3** To disable dynamic power assignment, choose **Fixed** under Tx Power Level Assignment and choose a default transmit power level from the drop-down box.

**Note** See Step 7 on page 11-31 for information on transmit power levels.

**Step 4** Click **Apply** to commit your changes.

**Step 5** Click **Save Configuration** to save your changes.

**Step 6** If you are overriding the default channel and power settings on a per radio basis, assign static channel and power settings to each of the access point radios that are joined to the controller.

**Step 7** If desired, repeat this procedure for the network type you did not select (802.11a or 802.11b/g).

## Using the CLI to Disable Dynamic Channel and Power Assignment

Follow these steps to disable RRM for all 802.11a or 802.11b/g radios.

**Step 1** Enter this command to disable the 802.11a or 802.11b/g network:

**config {802.11a | 802.11b} disable network**

**Step 2** Enter this command to disable RRM for all 802.11a or 802.11b/g radios and set all channels to the default value:

**config {802.11a | 802.11b} channel global off**

**Step 3** Enter this command to enable the 802.11a or 802.11b/g network:

**config {802.11a | 802.11b} enable network**

**Note** To enable the 802.11g network, enter **config 802.11b 11gSupport enable** after the **config 802.11b enable network** command.

**Step 4** Enter this command to save your settings:

**save config**

# Enabling Rogue Access Point Detection in RF Groups

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

## Using the GUI to Enable Rogue Access Point Detection in RF Groups

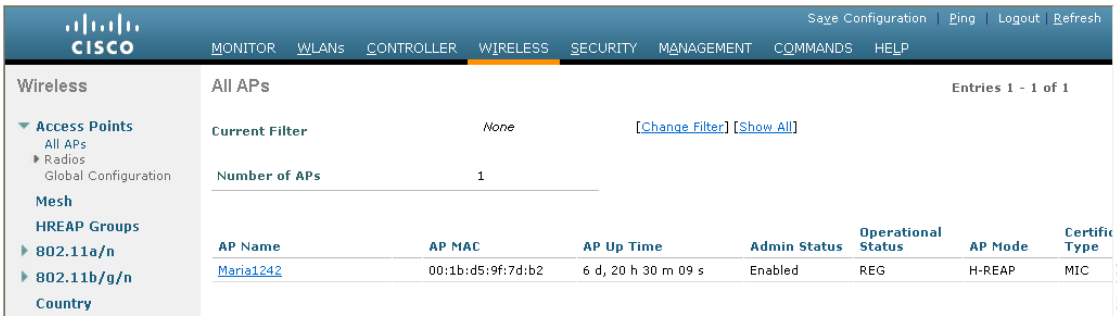
Using the controller GUI, follow these steps to enable rogue access point detection in RF groups.

**Step 1** Make sure that each controller in the RF group has been configured with the same RF group name.

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

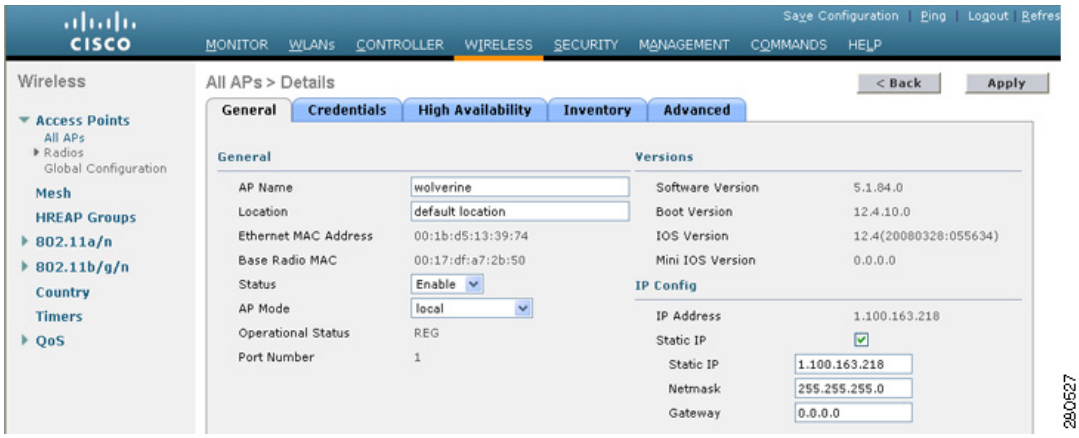
**Step 2** Choose **Wireless** to open the All APs page (see Figure 11-10).

***Figure 11-10 All APs Page***




**Step 3** Click the name of an access point to open the All APs > Details page (see Figure 11-11).

*Figure 11-11 All APs > Details Page*



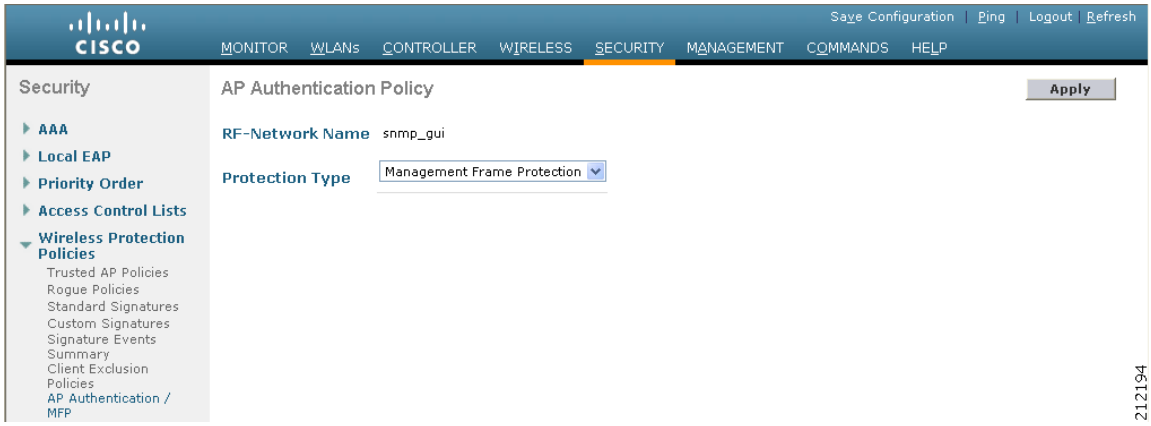

**Step 4** Choose either **local** or **monitor** from the AP Mode drop-down box and click **Apply** to commit your changes.

**Step 5** Click **Save Configuration** to save your changes.

**Step 6** Repeat Step 2 through Step 5 for every access point connected to the controller.

**Step 7** Choose **Security > Wireless Protection Policies > AP Authentication/MFP** to open the AP Authentication Policy page (see Figure 11-12).

*Figure 11-12 AP Authentication Policy Page*




The name of the RF group to which this controller belongs appears at the top of the page.

**Step 8** Choose **AP Authentication** from the Protection Type drop-down box to enable rogue access point detection.

**Step 9** Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

**Note** The valid threshold range is from1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

**Step 10** Click **Apply** to commit your changes.

**Step 11** Click **Save Configuration** to save your changes.

**Step 12** Repeat this procedure on every controller in the RF group.

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

# Using the CLI to Enable Rogue Access Point Detection in RF Groups

Using the controller CLI, follow these steps to enable rogue access point detection in RF groups.

**Step 1** Make sure that each controller in the RF group has been configured with the same RF group name.

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

**Step 2** Enter **config ap mode local** *Cisco_AP* or **config ap mode monitor** *Cisco_AP* to configure this particular access point for local (normal) mode or monitor (listen-only) mode.

**Step 3** Enter **save config** to save your settings.

**Step 4** Repeat Step 2 and Step 3 for every access point connected to the controller.

**Step 5** Enter **config wps ap-authentication** to enable rogue access point detection.

**Step 6** Enter **config wps ap-authentication** *threshold* to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

**Note** The valid threshold range is from1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

**Step 7** Enter **save config** to save your settings.

**Step 8** Repeat Step 5 through Step 7 on every controller in the RF group.

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

# Configuring Beamforming

Beamforming (also called *ClientLink*) is a spatial-filtering mechanism used at a transmitter to improve the received signal power or signal-to-noise (SNR) ratio at an intended receiver (client).

Cisco Aironet 1140 and 1250 series access points support beamforming. Beamforming uses multiple transmit antennas to focus transmissions in the direction of an 802.11a or 802.11g client, which increases the downlink SNR and the data rate to the client, reduces coverage holes, and enhances overall system performance. Beamforming works with all existing 802.11a and 802.11g clients.

Beamforming starts only when the signal from the client falls below these thresholds:

- **802.11a clients**—RSSI of –60 dBm or weaker
- **802.11g clients**—RSSI of –50 dBm or weaker

**Note** 802.11b clients do not support beamforming.

The access point actively maintains beamforming data for up to 15 clients per radio. These are the clients to which the access point is currently beamforming.

In the receive data path, the access point updates the beamforming data (the transmit steering matrix) for the active entries when packets are received from an address matching an active entry. If a packet is received from a beamforming client that is not an active entry, the access point automatically replaces the oldest active entry.

In the transmit data path, if the packet is destined for an active entry, the access point links the packets based on the recorded beamforming data.

## Guidelines for Using Beamforming

Follow these guidelines for using beamforming:

- Beamforming is supported only for legacy orthogonal frequency-division multiplexing (OFDM) data rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps).

  **Note** Beamforming is not supported for complementary code keying (CCK) data rates (1, 2, 5.5, and 11 Mbps).

- Only access points that support 802.11n (currently the 1140 and 1250 series access points) can use beamforming.
- Two or more antennas must be enabled for transmission.
- All three antennas must be enabled for reception.
- OFDM data rates must be enabled.
- Beamforming must be enabled.

**Note** If the antenna configuration restricts operation to a single transmit antenna or if OFDM data rates are disabled, beamforming is not used.

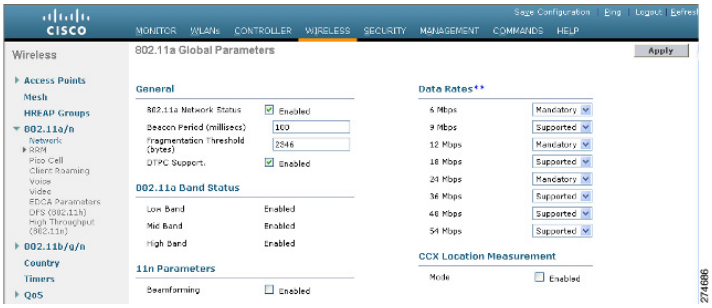
# Using the GUI to Configure Beamforming

Using the controller GUI, follow these steps to configure beamforming.

**Step 1** To disable the 802.11a or 802.11b/g network, follow these steps:

a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page (see Figure 11-13).

***Figure 11-13 802.11a Global Parameters Page***




b. Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 2** Check the **Beamforming** check box to globally enable beamforming on your 802.11a or 802.11g network, or leave it unchecked to disable this feature. The default value is disabled.

**Step 3** To re-enable the network, check the **802.11a** (or **802.11b/g**) **Network Status** check box.

**Step 4** Click **Apply** to commit your changes.

**Step 5** Click **Save Configuration** to save your changes.

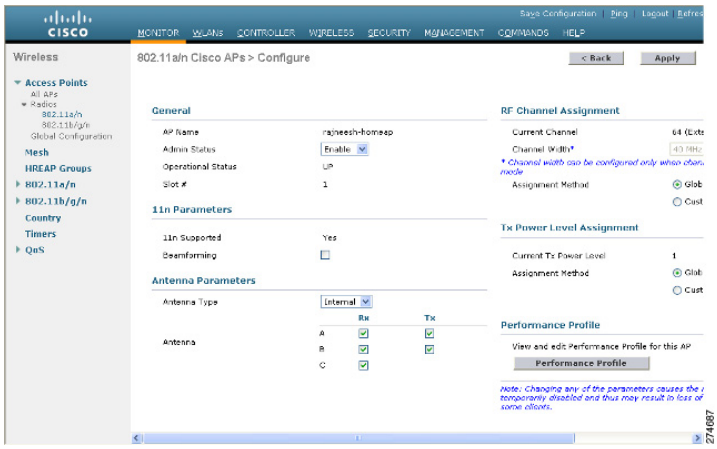
**Note** After you enable beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

**Step 6** If you want to override the global configuration and enable or disable beamforming for a specific access point, follow these steps:

a. Choose **Wireless > Access Points > Radios > 802.11a/n** or **802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.

b. Hover your cursor over the blue drop-down arrow for the access point for which you want to modify the radio configuration and choose **Configure**. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears (see Figure 11-14).

*Figure 11-14 802.11a/n Cisco APs > Configure Page*




**Step 7** In the 11n Parameters section, check the **Beamforming** check box to enable beamforming for this access point or leave it unchecked to disable this feature. The default value is unchecked if beamforming is disabled on the network and checked if beamforming is enabled on the network.

**Note** If the access point does not support 802.11n, the Beamforming option is not available.

**Step 8** Click **Apply** to commit your changes.

**Step 9** Click **Save Configuration** to save your changes.

# Using the CLI to Configure Beamforming

Using the controller CLI, follow these steps to configure beamforming.

**Step 1** To disable the 802.11a or 802.11b/g network, enter this command:

**config {802.11a | 802.11b} disable network**

**Step 2** To globally enable or disable beamforming on your 802.11a or 802.11g network, enter this command:

**config {802.11a | 802.11b} beamforming global {enable | disable}**

The default value is disabled.

**Note** After you enable beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

**Step 3** To override the global configuration and enable or disable beamforming for a specific access point, enter this command:

**config** {**802.11a** | **802.11b**} **beamforming ap** *Cisco_AP* **{enable | disable}**

The default value is disabled if beamforming is disabled on the network and enabled if beamforming is enabled on the network.

**Step 4** To re-enable the network, enter this command:

**config** {**802.11a** | **802.11b**} **enable network**

**Step 5** To save your changes, enter this command:

**save config**

**Step 6** To see the beamforming status for your network, enter this command:

**show** {**802.11a** | **802.11b**}

Information similar to the following appears:

```
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
...
Pico-Cell-V2 Status.......................... Disabled
TI Threshold................................. -50
Legacy Tx Beamforming setting................ Enabled
```

**Step 7** To see the beamforming status for a specific access point, enter this command:

**show ap config** {**802.11a** | **802.11b**} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 14
Cisco AP Name.................................... 1250-1
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
...
Phy OFDM parameters
      Configuration ............................. AUTOMATIC
      Current Channel ........................... 149
      Extension Channel ......................... NONE
      Channel Width.............................. 20 Mhz
      Allowed Channel List....................... 36,40,44,48,52,56,60,64,100,
        ......................................... 104,108,112,116,132,136,140,
        ......................................... 149,153,157,161,165
      TI Threshold .............................. -50
      Legacy Tx Beamforming Configuration ....... CUSTOMIZED
      Legacy Tx Beamforming ..................... ENABLED
```

# Configuring CCX Radio Management Features

You can configure two parameters that affect client location calculations:

- Radio measurement requests
- Location calibration

These parameters are supported in Cisco Client Extensions (CCX) v2 and higher and are designed to enhance location accuracy and timeliness for participating CCX clients. See the "Configuring Cisco Client Extensions" section on page 6-49 for more information on CCX.

For the location features to operate properly, the access points must be configured for normal, monitor, or hybrid-REAP mode. However, for hybrid-REAP mode, the access point must be connected to the controller.

**Note** CCX is not supported on the AP1030.

## Radio Measurement Requests

When this feature is enabled, lightweight access points issue broadcast radio measurement request messages to clients running CCXv2 or higher. The access points transmit these messages for every SSID over each enabled radio interface at a configured interval. In the process of performing 802.11 radio measurements, CCX clients send 802.11 broadcast probe requests on all the channels specified in the measurement request. The Cisco Location Appliance uses the uplink measurements based on these requests received at the access points to quickly and accurately calculate the client location. You do not need to specify on which channels the clients are to measure. The controller, access point, and client automatically determine which channels to use.

In controller software release 4.1 or later, the radio measurement feature has been expanded to enable the controller to also obtain information on the radio environment from the client's perspective (rather than from just that of the access point). In this case, the access points issue unicast radio measurement requests to a particular CCXv4 or v5 client. The client then sends various measurement reports back to the access point and onto the controller. These reports include information on the radio environment and data used to interpret the location of the clients. To prevent the access points and controller from being overwhelmed by radio measurement requests and reports, only two clients per access point and up to twenty clients per controller are supported. You can view the status of radio measurement requests for a particular access point or client as well as radio measurement reports for a particular client from the controller CLI.

Controller software release 4.1 or later also improves the ability of the Location Appliance to accurately interpret the location of a device through a new CCXv4 feature called location-based services. The controller issues a path-loss request to a particular CCXv4 or v5 client. If the client chooses to respond, it sends a path-loss measurement report to the controller. These reports contain the channel and transmit power of the client.

**Note** Non-CCX and CCXv1 clients simply ignore the CCX measurement requests and therefore do not participate in the radio measurement activity.

# Location Calibration

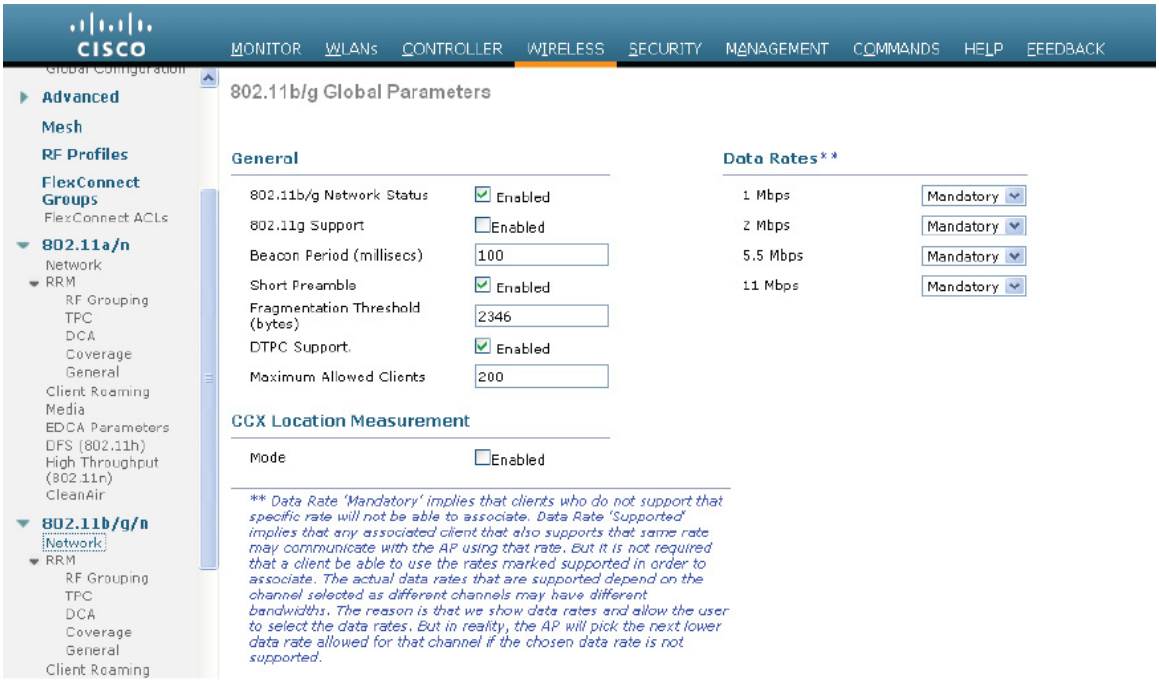
For CCX clients that need to be tracked more closely (for example, when a client calibration is performed), the controller can be configured to command the access point to send unicast measurement requests to these clients at a configured interval and whenever a CCX client roams to a new access point. These unicast requests can be sent out more often to these specific CCX clients than the broadcast measurement requests, which are sent to all clients. When location calibration is configured for non-CCX and CCXv1 clients, the clients are forced to disassociate at a specified interval to generate location measurements.

# Using the GUI to Configure CCX Radio Management

Follow these steps to configure CCX radio management using the controller GUI.

**Step 1** Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network**. The 802.11a (or 802.11b/g) Global Parameters page appears (see Figure 11-15).

***Figure 11-15 802.11a Global Parameters Page***




**Step 2** Under CCX Location Measurement, check the **Mode** check box to globally enable CCX radio management. This parameter causes the access points connected to this controller to issue broadcast radio measurement requests to clients running CCX v2 or higher. The default value is disabled (or unchecked).

**Step 3** If you checked the Mode check box in the previous step, enter a value in the Interval field to specify how often the access points are to issue the broadcast radio measurement requests.

**Range:** 60 to 32400 seconds

**Default:** 60 seconds

**Step 4** Click **Apply** to commit your changes.

**Step 5** Click **Save Configuration** to save your settings.

**Step 6** Follow the instructions in Step 2 of the "Using the CLI to Configure CCX Radio Management" section below to enable access point customization.

**Note** To enable CCX radio management for a particular access point, you must enable access point customization, which can be done only through the controller CLI.

**Step 7** If desired, repeat this procedure for the other radio band (802.11a or 802.11b/g).

# Using the CLI to Configure CCX Radio Management

Follow these steps to enable CCX radio management using the controller CLI.

**Step 1** To globally enable CCX radio management, enter this command:

**config advanced** {**802.11a** | **802.11b**} **ccx location-meas global enable** *interval_seconds*

The range for the *interval_seconds* parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes all access points connected to this controller in the 802.11a or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

**Step 2** To enable access point customization, enter these commands:

- **config advanced** {**802.11a** | **802.11b**} **ccx customize** *Cisco_AP* {**on** | **off**}

  This command enables or disables CCX radio management features for a particular access point in the 802.11a or 802.11b/g network.

- **config advanced** {**802.11a** | **802.11b**} **ccx location-meas ap** *Cisco_AP* **enable** *interval_seconds*

  The range for the *interval_seconds* parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes a particular access point in the 802.11a or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

**Step 3** To enable or disable location calibration for a particular client, enter this command:

**config client location-calibration** {**enable** | **disable**} *client _mac interval_seconds*

**Note** You can configure up to five clients per controller for location calibration.

**Step 4** To save your settings, enter this command:

**save config**

# Using the CLI to Obtain CCX Radio Management Information

Use these commands to obtain information about CCX radio management on the controller.

1. To see the CCX broadcast location measurement request configuration for all access points connected to this controller in the 802.11a or 802.11b/g network, enter this command:

   **show advanced** {**802.11a** | **802.11b**} **ccx global**

2. To see the CCX broadcast location measurement request configuration for a particular access point in the 802.11a or 802.11b/g network, enter this command:

   **show advanced** {**802.11a** | **802.11b**} **ccx ap** *Cisco_AP*

3. To see the status of radio measurement requests for a particular access point, enter this command:

   **show ap ccx rm** *Cisco_AP* **status**

   Information similar to the following appears:

```
A Radio

  Beacon Request.............................. Enabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Disabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration................................... 5

B Radio

  Beacon Request.............................. Disabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Enabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration................................... 5
```

4. To see the status of radio measurement requests for a particular client, enter this command:

   **show client ccx rm** *client_mac* **status**

   Information similar to the following appears:

```
Client Mac Address.......................... 00:40:96:ae:53:b4
Beacon Request.............................. Enabled
Channel Load Request........................ Disabled
Frame Request............................... Disabled
Noise Histogram Request..................... Disabled
Path Loss Request........................... Disabled
Interval.................................... 5
Iteration................................... 3
```

5. To see radio measurement reports for a particular client, enter these commands:

   - **show client ccx rm** *client_mac* **report beacon**—Shows the beacon report for the specified client.
   - **show client ccx rm** *client_mac* **report chan-load**—Shows the channel-load report for the specified client.

- **show client ccx rm** *client_mac* **report noise-hist**—Shows the noise-histogram report for the specified client.
- **show client ccx rm** *client_mac* **report frame**—Shows the frame report for the specified client.

6. To see the clients configured for location calibration, enter this command:

   **show client location-calibration summary**

7. To see the RSSI reported for both antennas on each access point that heard the client, enter this command:

   **show client detail** *client_mac*

## Using the CLI to Debug CCX Radio Management Issues

Use these commands if you experience any CCX radio management problems.

1. To debug CCX broadcast measurement request activity, enter this command:

   **debug airewave-director message** {**enable** | **disable**}

2. To debug client location calibration activity, enter this command:

   **debug ccxrm** [**all** | **error** | **warning** | **message** | **packet** | **detail** {**enable** | **disable**}]

3. The CCX radio measurement report packets are encapsulated in Internet Access Point Protocol (IAPP) packets. Therefore, if the previous **debug ccxrm** command does not provide any debugs, enter this command to provide debugs at the IAPP level:

   **debug iapp error {enable | disable}**

4. To debug the output for forwarded probes and their included RSSI for both antennas, enter this command:

   **debug dot11 load-balancing**

# Configuring Pico Cell Mode

In large multi-cell high-density wireless networks, it can be challenging to populate a site with a large number of access points to handle the desired cumulative bandwidth load while diminishing the contention between access points and maintaining quality of service. To optimize RF channel capacity and improve overall network performance, you can use the controller GUI or CLI to set high-density (or pico cell) mode parameters.

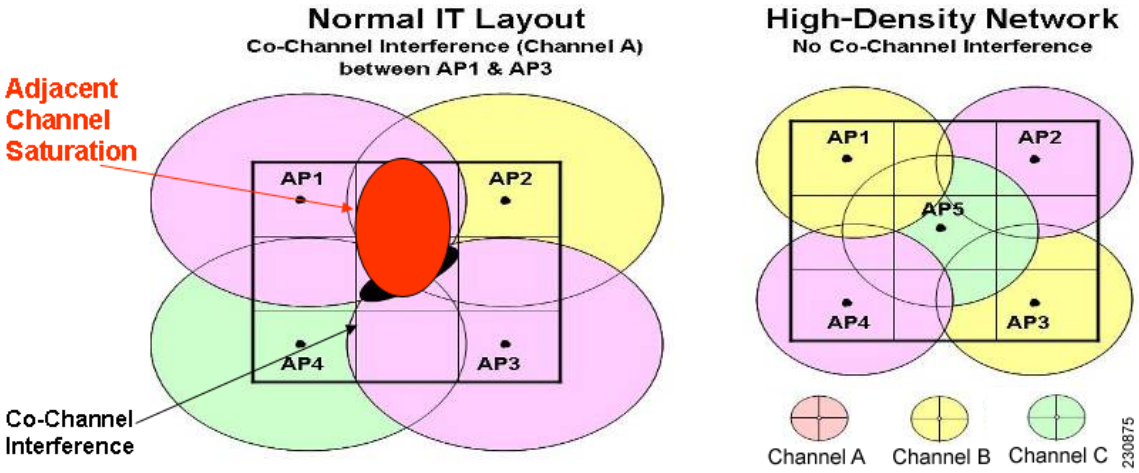
These parameters enable you to apply the same receiver sensitivity threshold, clear channel assessment (CCA) sensitivity threshold, and transmit power values across all access points registered to a given controller. When a client that supports high density associates to an access point with high density enabled, they exchange specific 802.11 information elements (IEs) that instruct the client to adhere to the access point's advertised receive sensitivity threshold, CCA sensitivity threshold, and transmit power values. These three parameters reduce the effective cell size by adjusting the received signal strength before an access point and client consider the channel accessible for the transfer of packets. When all access points and clients raise the signal standard in this way throughout a high-density area, access points can be deployed closer together without interfering with each other or being overwhelmed by environmental and distant-rogue signals.

The benefits of a high-density-enabled wireless network include the following:

- Most efficient use of the available spectrum
- Significant increase in aggregate client throughput or throughput per square feet
- Significant increase in wireless LAN capacity
- Linear capacity growth
- Higher interference tolerance by allowing WiFi to transmit over top of the interference

Figure 11-16 shows an example of a high-density network.

*Figure 11-16 High-Density Network Example*




# Guidelines for Using Pico Cell Mode

Follow these guidelines for using pico cell mode:

- High-density networking is supported on Cisco lightweight access points and on notebooks using the Intel PRO/Wireless 3945ABG and Intel Wireless WiFi Link 4965AG clients.
- In order to use pico cell mode version 2, the WMM policy for the Intel clients must be set to Allowed.
- To support high-density, both the client s and access points must be configured for high density. Do not mix high-density and non-high-density devices in the same network.
- High-density access points must be joined to a dedicated controller.
- When you adjust the pico cell mode parameters, the following RRM values automatically change:
  - The default value of the Fixed option for the Power Level Assignment Method parameter [on the 802.11a (or 802.11b) > RRM > Tx Power Control (TPC) page] reflects the power setting that you specify for the pico cell Transmit Power parameter.
  - The default value of the Power Threshold parameter [on the 802.11a (or 802.11b) > RRM > Tx Power Control (TPC) page] reflects the value that you specify for the pico cell CCA Sensitivity Threshold parameter.

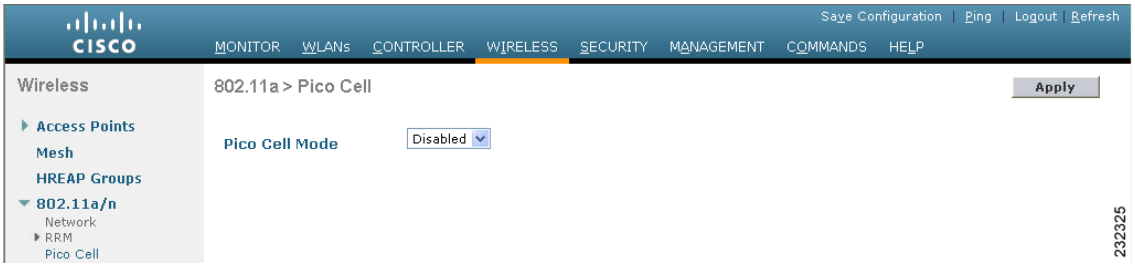
# Using the GUI to Configure Pico Cell Mode

Follow these steps to configure pico cell mode using the controller GUI.

**Step 1** Disable the 802.11a or 802.11b/g network before changing pico cell mode parameters. To do so, choose **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Network** and uncheck the **802.11a Network Status** (or **802.11b/g Network Status**) check box.

**Step 2** Choose **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Pico Cell** to open the 802.11a (or 802.11b/g) > Pico Cell page (see Figure 11-17).

***Figure 11-17 802.11a > Pico Cell Page***

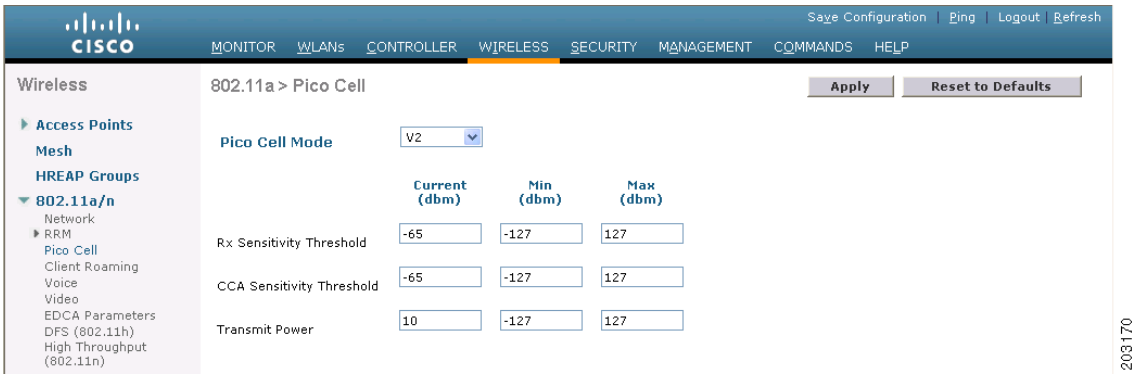



**Step 3** Choose one of these options from the Pico Cell Mode drop-down box:

- **Disable**—Disables pico cell mode. This is the default value.
- **V1**—Enables pico cell mode version 1. This option is designed for use with legacy Airespace products (those released prior to Cisco's acquisition of Airespace). Cisco recommends that you choose V2 if you want to enable pico cell mode.
- **V2**—Enables pico cell mode version 2. Choose this option if you want to adjust the pico cell mode parameters to optimize network performance in high-density areas, where all the clients support high density.

**Step 4** If you chose V2 in Step 3, the 802.11a (or 802.11b/g) > Pico Cell page displays three configurable fields: Rx Sensitivity Threshold, CCA Sensitivity Threshold, and Transmit Power (see Figure 11-18).

***Figure 11-18 802.11a > Pico Cell Page with Pico Cell Mode V2 Parameters***




Use the information in Table 11-3 to adjust the values of these parameters as necessary.

**Note** The default values for these parameters should be appropriate for most applications. Therefore, Cisco recommends that you use the default values.

*Table 11-3 Pico Cell Mode V2 Parameters*

| Parameter | Description |
|---|---|
| Rx Sensitivity Threshold | Specifies the current, minimum, and maximum values (in dBm) for the receiver sensitivity of the 802.11a or 802.11b/g radio. The current value sets the receiver sensitivity on the local radio. The min and max values are used only for inclusion in the Inter-Access Point Protocol (IAPP) high-density reports.<br>**Default:** –65 dBm (Current), –127 dBm (Min), and 127 dBm (Max) |
| CCA Sensitivity Threshold | Specifies the clear channel assessment (CCA) sensitivity threshold on all radios in the high-density cell. The current value programs the 802.11a or 802.11b/g receiver. The min and max values are for advertisement in IAPP reports.<br>**Default:** –65 dBm (Current), –127 dBm (Min), and 127 dBm (Max) |
| Transmit Power | Specifies the high-density transmit power used by both the access point and client 802.11a or 802.11b/g radios.<br>**Default:** 10 dBm (Current), –127 dBm (Min), and 127 dBm (Max) |

**Note** The min and max values in Figure 11-18 and Table 11-3 are used only to indicate the range to the client. They are not used on the access point.

**Step 5** Click **Apply** to commit your changes.

**Step 6** Re-enable the 802.11a or 802.11b/g network. To do so, choose **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Network** and check the **802.11a Network Status** (or **802.11b/g Network Status**) check box.

**Step 7** Click **Save Configuration** to save your changes.

**Note** If you change the values of the pico cell mode parameters and later want to reset them to their default values, click **Reset to Defaults** and then click **Apply**.

# Using the CLI to Configure Pico Cell Mode

**Note** Refer to the "Using the GUI to Configure Pico Cell Mode" section on page 11-49 for descriptions and default values of the parameters used in the CLI commands.

**Step 1** To disable the 802.11a or 802.11b/g network before changing pico cell mode parameters, enter this command:

**config {802.11a | 802.11b} disable**

**Step 2** To enable pico cell mode, enter one of these commands:

- **config {802.11a | 802.11b} picocell enable**—Enables pico cell mode version 1. This command is designed for use with a specific application. Cisco recommends that you use the **config {802.11a | 802.11b} picocell-V2 enable** command if you want to enable pico cell mode.
- **config {802.11a | 802.11b} picocell-V2 enable**—Enables pico cell mode version 2. Use this command if you want to adjust the pico cell mode parameters to optimize network performance in high-density areas.

**Step 3** If you enabled pico cell mode version 2 in Step 2, follow these steps to configure the receive sensitivity threshold, CCA sensitivity threshold, and transmit power parameters:

a. To configure the receive sensitivity threshold, enter this command:

**config advanced {802.11a | 802.11b} receiver pico-cell-V2 rx_sense_threshold** *min max current*

b. To configure the CCA sensitivity threshold, enter this command:

**config advanced {802.11a | 802.11b} receiver pico-cell-V2 cca_sense_threshold** *min max current*

c. To configure the transmit power, enter this command:

**config advanced {802.11a | 802.11b} receiver pico-cell-V2 sta_tx_pwr** *min max current*

**Step 4** If you enabled pico cell mode version 2 in Step 2 and you want to transmit a unicast IAPP high-density frame request to a specific client, enter this command:

**config advanced {802.11a | 802.11b} receiver pico-cell-V2 send_iapp_req** *client_mac*

**Step 5** To re-enable the 802.11a or 802.11b/g network, enter this command:

**config {802.11a | 802.11b} enable**

**Step 6** To save your settings, enter this command:

**save config**

# Using the CLI to Debug Pico Cell Mode Issues

Use these commands if you experience any pico cell mode problems.

1. To see the current status of pico cell mode, enter this command:

   **show {802.11a | 802.11b}**

   Information similar to the following appears:

```
802.11a Network.............................. Disabled
11nSupport................................... Disabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
...
Pico-Cell Status............................. Disabled
Pico-Cell-V2 Status.......................... Enabled
```

2. To see the receiver parameters that are set by the pico cell mode commands, enter this command:

   **show advanced {802.11a | 802.11b} receiver**

   Information similar to the following appears:

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 30
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 30
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Disabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Disabled
 TxStomp  : Wrong BSSID Data Only Status......... Disabled
 RxAbort  : Raw Power Drop Status................ Disabled
 RxAbort  : Raw Power Drop Threshold............. 10
 RxAbort  : Low RSSI Status...................... Disabled
 RxAbort  : Low RSSI Threshold................... 30
 RxAbort  : Wrong BSSID Status................... Disabled
 RxAbort  : Wrong BSSID Data Only Status......... Disabled
 ----------------------------------------....
 pico-cell-V2 parameters in dbm units:
 RxSensitivity: Min,Max,Current RxSense Thres.... -127,127,-65
 CCA Threshold: Min,Max,Current Clear Channel.... -127,127,-65
Tx Pwr: Min,Max,Current Transmit Power for A..... -127,127,10
 ----------------------------------------....
```

3. To see the noise and interference information, coverage information, client signal strengths and signal-to-noise ratios, and nearby access points, enter this command:

   **show ap auto-rf {802.11a | 802.11b}** *Cisco_AP*

   Information similar to the following appears:

```
Number Of Slots................................. 2
AP Name......................................... AP1242.47b2.31f6
MAC Address..................................... 00:16:47:b2:31:f6
  Radio Type.................................... RADIO_TYPE_80211a
  Noise Information
    Noise Profile............................... PASSED
  Interference Information
    Interference Profile........................ PASSED
  Load Information
    Load Profile................................ PASSED
    Receive Utilization......................... 0 %
    Transmit Utilization........................ 0 %
    Channel Utilization......................... 0 %
    Attached Clients............................ 0 clients
  Coverage Information
    Coverage Profile............................ PASSED
    Failed Clients.............................. 0 clients
  Client Signal Strengths
    RSSI -100 dbm............................... 0 clients
    RSSI  -92 dbm............................... 0 clients
    RSSI  -84 dbm............................... 0 clients
    RSSI  -76 dbm............................... 0 clients
    RSSI  -68 dbm............................... 0 clients
    RSSI  -60 dbm............................... 0 clients
    RSSI  -52 dbm............................... 0 clients
```

```
Client Signal To Noise Ratios
  SNR    0 dB.............................. 0 clients
  SNR    5 dB.............................. 0 clients
  SNR   10 dB.............................. 0 clients
  SNR   15 dB.............................. 0 clients
  SNR   20 dB.............................. 0 clients
  SNR   25 dB.............................. 0 clients
  SNR   30 dB.............................. 0 clients
  SNR   35 dB.............................. 0 clients
  SNR   40 dB.............................. 0 clients
  SNR   45 dB.............................. 0 clients
Nearby APs
Radar Information
RF Parameter Recommendations
  Power Level.............................. 0
  RTS/CTS Threshold........................ 0
  Fragmentation Threshold.................. 0
  Antenna Pattern.......................... 0
```