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 RF Groups, page 10-5
- Configuring an RF Group, page 10-6
- Viewing RF Group Status, page 10-8
- Enabling Rogue Access Point Detection, page 10-12
- Configuring Dynamic RRM, page 10-15
- Overriding Dynamic RRM, page 10-23
- Viewing Additional RRM Settings Using the CLI, page 10-28
- Configuring CCX Radio Management Features, page 10-29
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 access points**—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
- Dynamic channel assignment
- Dynamic transmit power control
- Coverage hole detection and correction
- Client and network load balancing

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 point goes “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.

If packets have been in the voice queue in the last 100 ms, the access point does not go off-channel.

By default, 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.
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 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.
Overview of Radio Resource Management

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.

Dynamic 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 access points such that they see their fourth strongest neighbor at an optimal –65 dbm or better.

The transmit power control algorithm only reduces an access point’s power. However, the coverage hole algorithm, explained below, can increase access point power, thereby filling a coverage hole. For example, if a failed access point is detected, the coverage hole algorithm can automatically increase power on surrounding access points to fill the gap created by the loss in coverage.

Note

See Step 5 on page 10-25 for an explanation of the transmit power levels.

Coverage Hole Detection and Correction

RRM’s coverage hole detection 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 signal-to-noise ratio (SNR) levels that are lower than the thresholds specified in the Auto RF 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 administrator can look up the historical record of access points to see if these alerts are chronic, indicating the existence of a persistent coverage hole as opposed to an isolated problem.

Client and Network Load Balancing

RRM load-balances new clients across grouped lightweight access points reporting to each controller. This function is particularly important when many clients converge in one spot (such as a conference room or auditorium) because RRM can automatically force some subscribers to associate with nearby access points, allowing higher throughput for all clients. The controller provides a centralized view of client loads on all access points. This information can be used to influence where new clients attach to the network or to direct existing clients to new access points to improve wireless LAN performance. The result is an even distribution of capacity across an entire wireless network.

Note

Client load balancing works only for a single controller. It is not operate in a multi-controller environment.
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 the monitor intervals specified in Table 10-1, 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.

Note
RRM measurements are postponed on a per access point basis where traffic remains in the platinum QoS queue, if there was voice traffic in the last 100 ms.

Overview of RF Groups

An RF group, also known as an RF domain, is a cluster of controllers that coordinates its dynamic 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. The RRM algorithms use a shared secret that is configured on the controller and sent to each access point. Access points sharing the same secret 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 Chapter 11 for more information on mobility groups.

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 group leader is dynamically chosen and cannot be selected by the user. In addition, the RF group leader can change at any time, depending on the RRM algorithm calculations.
The RF group leader analyzes real-time radio data collected by the system and calculates the master power and channel plan. The RRM algorithms try to optimize around a signal strength of –65 dBm between all access points and to avoid 802.11 co-channel interference and contention as well as non-802.11 interference. The RRM algorithms employ dampening calculations to minimize system-wide dynamic changes. The end result is dynamically calculated optimal power and channel planning that is responsive to an always changing RF environment.

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 Table 10-1 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. You can include up to 20 controllers and 1000 access points in an RF group.

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

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**  Click **Controller > General** to access the General page (see **Figure 10-1**).

![Figure 10-1  General Page](image)

**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 Click Wireless to access the All APs page (see Figure 10-2).
Step 2  
Under 802.11a or 802.11b/g, click **Network** to access the 802.11a (or 802.11b/g) Global Parameters page (see Figure 10-3).

**Figure 10-3  802.11a Global Parameters Page**

Step 3  
Click **Auto RF** to access the 802.11a (or 802.11b/g) Global Parameters > Auto RF page (see Figure 10-4).
Figure 10-4 802.11a Global Parameters > Auto RF Page

- **Group Mode**: Enabled
- **Group Update Interval**: 600 secs
- **Group Leader**: 08:11:92:ff:88:dd
- **Is this Controller a Group Leader?**: Yes
- **Last Group Update**: 367 secs ago

**RF Channel Assignment**

- **Channel Assignment Method**: Automatic
- **Avoid Foreign AP Interference**: Enabled
- **Avoid Cisco AP Interference**: Enabled
- **Avoid Non-802.11a noise**: Enabled
- **Signal Strength Contribution**: Enabled
- **Channel Assignment Leader**: 08:11:92:ff:88:dd
- **Last Auto Channel Assignment**: 367 secs ago

**Tx Power Level Assignment**

- **Power Level Assignment Method**: Automatic
- **Power Threshold**: -65 dbm
- **Power Neighbor Count**: 3
- **Power Update Count**: 3
- **Power Assignment Leader**: 08:11:92:ff:88:dd
- **Last Power Level Assignment**: 367 secs ago

**Profile Thresholds**

- **Interference (0 to 100%)**: 12
- **Client (1 to 75%)**: 12
- **Noise (-127 to 0 dbm)**: -79
- **Coverage 3 to 50 dbm**: 16
- **Utilization (0 to 100%)**: 80
- **Coverage Exception Level (0 to 100%)**: 15
- **Date Rate 1 to 1300 Kbps**: 1000
- **Client Min Exception Level (1 to 75%)**: 3

**Noise/Interference/Rogue Monitoring Channels**

- **Channel List**: Country Channels

**Monitor Intervals** (60 to 3600 secs)

- **Noise Measurement**: 180
- **Load Measurement**: 60
- **Signal Measurement**: 60
- **Coverage Measurement**: 180

**Factory Default**

Set all Auto RF 802.11a parameters to Factory Default.

146927
The top of 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 Table 10-1 for more information on this parameter.

**Step 4** 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.
Enabling Rogue Access Point Detection

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

Follow these steps to enable rogue access point detection using the GUI.

**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** Click **Wireless** to access the All APs page (see Figure 10-5).

**Figure 10-5 All APs Page**

<table>
<thead>
<tr>
<th>Access Points</th>
<th>Search by Ethernet MAC</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>All APs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All APs</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>Mesh</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>AddOrUpdate</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>802.11e Voice</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>802.11b/g</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>Country</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
<tr>
<td>Timers</td>
<td>00:16:5a:69:1c:06</td>
<td>REG</td>
</tr>
</tbody>
</table>
**Step 3**  
Click the **Detail** link for an access point to access the All APs > Details page (see **Figure 10-6**).

**Figure 10-6  All APs > Details Page**

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>00:10:00:00:00:10</td>
</tr>
<tr>
<td>Ethernet MAC Address</td>
<td>00:0b:86:5f:be:90</td>
</tr>
<tr>
<td>Base Radio MAC</td>
<td>00:0b:86:5f:be:90</td>
</tr>
<tr>
<td>Regulatory Domain</td>
<td>60211bg - A 60211bg - A</td>
</tr>
<tr>
<td>AP ID</td>
<td>10.70.0.113</td>
</tr>
<tr>
<td>AP Mode</td>
<td>local</td>
</tr>
<tr>
<td>Mirror Mode</td>
<td>Disable</td>
</tr>
<tr>
<td>AP Group Name</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>default location</td>
</tr>
<tr>
<td>Primary Controller Name</td>
<td></td>
</tr>
<tr>
<td>Secondary Controller Name</td>
<td></td>
</tr>
<tr>
<td>Teritary Controller Name</td>
<td></td>
</tr>
<tr>
<td>Statistics Timer</td>
<td>100</td>
</tr>
</tbody>
</table>

**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**  
Click **Security > AP Authentication/MFP** (under Wireless Protection Policies) to access the AP Authentication Policy page (see **Figure 10-7**).

**Figure 10-7  AP Authentication Policy Page**

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Authentication Policy</td>
<td></td>
</tr>
<tr>
<td>RF-Network Name</td>
<td>DC-1</td>
</tr>
<tr>
<td>Protection Type</td>
<td>AP Authentication</td>
</tr>
<tr>
<td>Alarm Trigger Threshold</td>
<td>1</td>
</tr>
</tbody>
</table>

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 from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

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

Follow these steps to enable rogue access point detection using the CLI.

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 from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.
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 Dynamic RRM

The controller is preconfigured with factory default RRM settings designed to optimize radio performance. However, you can modify the controller’s dynamic RRM configuration parameters at any time through either the GUI or the CLI.

**Note**  You can configure these parameters on an individual controller that is not part of an RF group or on RF group members.

**Note**  The RRM parameters should be set to the same values on every controller in an RF group. The RF group leader can change at any time. 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 Dynamic RRM

Follow these steps to configure dynamic RRM parameters using the GUI.

Step 1  Access the 802.11a (or 802.11b/g) Global Parameters > Auto RF page (see Figure 10-4).

---

**Note**  Click `Set to Factory Default` at the bottom of the page if you want to return all of the controller’s RRM parameters to their factory default values.
Step 2  Table 10-1 lists and describes the configurable RRM parameters. Follow the instructions in the table to make any desired changes.

**Table 10-1  RRM Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Group</td>
<td></td>
</tr>
<tr>
<td>Group Mode</td>
<td>Determines whether the controller participates in an RF group. Options: Enabled or Disabled Default: Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>The controller automatically forms an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings for the group.</td>
</tr>
<tr>
<td>Disabled</td>
<td>The controller does not participate in automatic RF grouping. Rather, it optimizes its own access point parameters.</td>
</tr>
</tbody>
</table>

**Note**  Cisco recommends that controllers participate in automatic RF grouping. However, you can disable this feature if necessary by unchecking the check box. Note also, however, that you override dynamic RRM settings without disabling automatic RF group participation. See the “Overriding Dynamic RRM” section on page 10-23 for instructions.
Table 10-1  RRM Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Channel Assignment</td>
<td>The controller’s dynamic channel assignment mode.</td>
</tr>
<tr>
<td>Channel Assignment</td>
<td>Options: Automatic, On Demand, or Off</td>
</tr>
<tr>
<td>Method</td>
<td>Default: Automatic</td>
</tr>
<tr>
<td></td>
<td><strong>Channel Assignment Method</strong></td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Automatic Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined access points.</td>
</tr>
<tr>
<td></td>
<td>On Demand Causes the controller to periodically evaluate the channel assignment for all joined access points. However, the controller reassigns channels, if necessary, only when you click <strong>Invoke Channel Update Now</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The controller does not evaluate and update the channel immediately after you click Invoke Channel Update Now. It waits for the next interval (default is 600 seconds).</td>
</tr>
<tr>
<td></td>
<td>Off Prevents the controller from evaluating and, if necessary, updating the channel assignment for joined access points.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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 10-27 for instructions if you ever need to disable the controller’s dynamic settings.</td>
</tr>
<tr>
<td>Avoid Foreign AP</td>
<td>Causes 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. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points.</td>
</tr>
<tr>
<td>Interference</td>
<td>Options: Enabled or Disabled</td>
</tr>
<tr>
<td></td>
<td>Default: Enabled</td>
</tr>
</tbody>
</table>
### Configuring Dynamic RRM

Avoid Cisco AP Load

Causes the controller’s RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load.

**Options:** Enabled or Disabled  
**Default:** Disabled

Avoid Non-802.11 (802.11b) Noise

Causes the controller’s RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points. For example, RRM may have access points avoid channels with significant interference from non-access point sources, such as microwave ovens.

**Options:** Enabled or Disabled  
**Default:** Enabled

The following non-configurable RF channel parameter settings are also shown:

- **Signal Strength Contribution**—This parameter is always enabled. RRM constantly monitors the relative location of all access points within the RF group to ensure near-optimal channel reuse.

- **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.

---

#### Table 10-1 RRM Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Avoid Cisco AP Load                | Causes the controller’s RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. **Options:** Enabled or Disabled  
**Default:** Disabled |
| Avoid Non-802.11 (802.11b) Noise   | Causes the controller’s RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points. For example, RRM may have access points avoid channels with significant interference from non-access point sources, such as microwave ovens.  
**Options:** Enabled or Disabled  
**Default:** Enabled |
### Table 10-1  RRM Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tx Power Level Assignment</strong></td>
<td>The controller’s dynamic power assignment mode. <strong>Options:</strong> Automatic, On Demand, or Fixed  <strong>Default:</strong> Automatic</td>
</tr>
<tr>
<td><strong>Power Level Assignment</strong> Method</td>
<td><strong>Automatic:</strong> Causes the controller to periodically evaluate and, if necessary, update the transmit power for all joined access points. <strong>On Demand:</strong> 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 <strong>Invoke Power Update Now</strong>. <strong>Note:</strong> The controller does not evaluate and update the transmit power immediately after you click <strong>Invoke Power Update Now</strong>. It waits for the next interval (default is 600 seconds). <strong>Fixed:</strong> 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. <strong>Note:</strong> 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 <strong>Step 5 on page 10-25</strong> for information on available transmit power levels. <strong>Note:</strong> 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 10-27 for instructions if you ever need to disable the controller’s dynamic settings.</td>
</tr>
</tbody>
</table>

---

**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 5 on page 10-25** for information on available transmit power levels.
Configuring Dynamic RRM

The following non-configurable transmit power level parameter settings are also shown:

- **Power Threshold** and **Power Neighbor Count**—These parameters are used to fine tune the power control. The objective is to limit power so that at most the neighbor count access points receive the signal of each access point above a power threshold.

- **Power Update Contribution**—The factors used for changing power assignment levels: load (L), signal (S), noise (N), or interference (I).

- **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.

**Profile Thresholds**—Lightweight access points send an SNMP trap (or an alert) to the controller when the values set for these threshold parameters are exceeded. The controller’s RRM software uses this information to evaluate the integrity of the entire network and makes adjustments accordingly.

### Table 10-1 RRM Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interference (0 to 100%)</td>
<td>The percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. Default: 10%</td>
</tr>
<tr>
<td>Clients (1 to 75)</td>
<td>The number of clients on a single access point. Default: 12</td>
</tr>
<tr>
<td>Noise (-127 to 0 dBm)</td>
<td>The level of noise (non-802.11 traffic) on a single access point. Default: -70 dBm</td>
</tr>
<tr>
<td>Coverage (3 to 50 dB)</td>
<td>The signal-to-noise ratio (SNR) per access point. This value is also used for reporting detected coverage holes. Default: 12 dB (802.11b/g) or 16 dB (802.11a)</td>
</tr>
<tr>
<td>Utilization (0 to 100%)</td>
<td>The percentage of RF bandwidth being used by a single access point. Default: 80%</td>
</tr>
<tr>
<td>Coverage Exception Level (0 to 100%)</td>
<td>The percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. This value is based on the Coverage threshold and the Client Min Exception Level threshold. Default: 25%</td>
</tr>
<tr>
<td>Data Rate (1 to 1000 Kbps)</td>
<td>The rate at which a single access point transmits or receives data packets. Default: 1000 Kbps</td>
</tr>
</tbody>
</table>
### Table 10-1  RRM Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Client Min Exception Level (1 to 75) | The minimum number of clients on an access point with a signal-to-noise ratio (SNR) below the Coverage threshold. This threshold works in conjunction with the Coverage and Coverage Exception Level thresholds. A coverage exception is alerted if the Coverage Exception Level percentage of clients (25%) and the Client Min Exception Level number of clients (3) fall below the Coverage threshold (12 dB). In this example, a coverage alarm would be generated if at least 25% and a minimum of 3 clients have an SNR value below 12 dB (802.11b/g) or 16 dB (802.11a).  
**Default:** 3 |

**Noise/Interference/Rogue Monitoring Channels**

<table>
<thead>
<tr>
<th>Channel List</th>
<th>Description</th>
</tr>
</thead>
</table>
| Channel List | The set of channels that the access point uses for RRM scanning.  
**Options:** All Channels, Country Channels, or DCA Channels  
**Default:** Country Channels |

<table>
<thead>
<tr>
<th>Channel List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Channels</td>
<td>RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.</td>
</tr>
<tr>
<td>Country Channels</td>
<td>RRM channel scanning occurs only on the data channels in the country of operation.</td>
</tr>
</tbody>
</table>
| DCA Channels | RRM channel scanning occurs only on the channel set used by the dynamic channel allocation (DCA) algorithm, which typically includes all the non-overlapping channels allowed in the country of operation.  
**Note** You can specify the channel set to be used for DCA from the controller CLI. See the “Using the CLI to Configure Dynamic RRM” section on page 10-22 for instructions. |

**Monitor Intervals**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Noise Measurement | How frequently the access point measures noise and interference.  
**Range:** 60 to 3600 seconds  
**Default:** 180 seconds |
| Load Measurement | How frequently the access point measures 802.11 traffic.  
**Range:** 60 to 3600 seconds  
**Default:** 60 seconds |
### Configuring Dynamic RRM

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

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

#### Step 5
Repeat this procedure to set the same parameter values for every controller in the RF group.

#### Using the CLI to Configure Dynamic RRM

Follow these steps to configure dynamic RRM using the CLI.

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

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

#### Step 2
Perform one of the following:

- 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 specify the channel set used for dynamic channel allocation, 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.

---

**Table 10-1 RRM Parameters (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal Measurement</td>
<td>How frequently the access point measures signal strength and how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 60 to 3600 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 60 seconds</td>
</tr>
<tr>
<td>Coverage Measurement</td>
<td>How frequently the access point measures the coverage area and passes this information to the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 60 to 3600 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 180 seconds</td>
</tr>
</tbody>
</table>
Step 3 Perform one of the following:

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

  \[\text{config} \{802.11a | 802.11b\} \text{ txPower global auto}\]

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

  \[\text{config} \{802.11a | 802.11b\} \text{ txPower global once}\]

Step 4 Enter this command to enable the 802.11a or 802.11b/g network:

\[\text{config} \{802.11a | 802.11b\} \text{ enable}\]

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

Step 5 Enter this command to save your settings:

\[\text{save config}\]

---

**Overriding Dynamic RRM**

In some deployments, it is desirable to statically assign channel and transmit power settings to the access points instead of relying on the dynamic 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 10-24
- Disabling Dynamic Channel and Power Assignment Globally for a Controller, page 10-27

**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.

**Note** You can also override dynamic RRM using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.
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
Click Wireless to access the All APs page (see Figure 10-2).

Step 2
Under Access Points, click either 802.11a Radios or 802.11b/g Radios to access the 802.11a (or 802.11b/g) Radios page (see Figure 10-8).

Figure 10-8  802.11a Radios Page

This page shows all the 802.11a or 802.11b/g access point radios that are joined to the controller and their current settings.
Step 3  Click **Configure** for the access point for which you want to modify the radio configuration. The 802.11a (or 802.11b/g) Cisco APs > Configure page appears (see Figure 10-9).

**Figure 10-9  802.11a Cisco APs > Configure Page**

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.

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.

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

Step 5  Click **Save Configuration** to save the changes to the access point radio.

Step 6  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** Enter this command to disable the 802.11a or 802.11b/g network:
```
config {802.11a | 802.11b} disable
```

**Step 2** To specify the channel that a particular access point is to use, enter this command:
```
config {802.11a | 802.11b} channel Cisco_AP channel
```
Example: To configure 802.11a channel 36 as the default channel on AP1, enter this command:
```
config 802.11a channel AP1 36.
```

**Step 3** To specify the transmit power level that a particular access point is to use, enter this command:
```
config {802.11a | 802.11b} txPower 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 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 4** Enter this command to save your settings:
```
save config
```

**Step 5** Repeat Step 2 through Step 4 for each access point radio for which you want to assign a static channel and power level.

**Step 6** Enter this command to enable the 802.11a or 802.11b/g network:
```
config {802.11a | 802.11b} enable
```

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

**Step 7** Enter this command to save your settings:
```
save config
```
Disabling Dynamic Channel and Power Assignment Globally for a Controller

You can use the GUI or CLI to disable dynamic channel and power assignment.

Using the GUI to Disable Dynamic Channel and Power Assignment

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

1. **Step 1** Click **Wireless** to access the All APs page (see Figure 10-2).
2. **Step 2** Under 802.11a or 802.11b/g, click **Network** to access the 802.11a (or 802.11b/g) Global Parameters page (see Figure 10-3).
3. **Step 3** Click **Auto RF** to access the 802.11a (or 802.11b/g) Global Parameters > Auto RF page (see Figure 10-4).
4. **Step 4** To disable dynamic channel assignment, choose **Off** under RF Channel Assignment.
5. **Step 5** 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 5 on page 10-25 for information on transmit power levels.

6. **Step 6** Click **Apply** to commit your changes.
7. **Step 7** Click **Save Configuration** to save your changes.
8. **Step 8** 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.
9. **Step 9** 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.

1. **Step 1** Enter this command to disable the 802.11a or 802.11b/g network:
   ```
   config {802.11a | 802.11b} disable
   ```
2. **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
   ```
3. **Step 3** Enter this command to enable the 802.11a or 802.11b/g network:
   ```
   config {802.11a | 802.11b} enable
   ```

Note: To enable the 802.11g network, enter `config 802.11b 11gSupport enable` after the `config 802.11b enable` command.
Step 4 Enter this command to save your settings:

    save config

Viewing Additional RRM Settings Using the CLI

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

- `show advanced 802.11a ?`
- `show advanced 802.11b ?`

where `?` is one of the following:

- `ccx`—Shows the Cisco Compatible Extensions (CCX) RRM configuration.
- `channel`—Shows the channel assignment configuration and statistics.
- `logging`—Shows the RF event and performance logging.
- `monitor`—Shows the Cisco radio monitoring.
- `profile`—Shows the access point performance profiles.
- `receiver`—Shows the 802.11a or 802.11b/g receiver configuration and statistics.
- `summary`—Shows the configuration and statistics of the 802.11a or 802.11b/g access points
- `txpower`—Shows the transmit power assignment configuration and statistics.

Note To troubleshoot RRM-related issues, refer to the Cisco Wireless LAN Controller Command Reference, Release 3.2 for RRM (airwave-director) debug commands.
Chapter 10  Configuring Radio Resource Management

Configuring CCX Radio Management Features

In controller software release 4.0, you can configure two parameters that affect client location calculations:

- Broadcast location 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 Quality of Service Profiles” section on page 6-19 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.

Broadcast Location 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 location 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.

Note: Non-CCX and CCXv1 clients simply ignore the CCX measurement requests and therefore do not participate in this location 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 Click **Wireless** and then click **Network** under either 802.11a or 802.11b/g. The 802.11a (or 802.11b/g) Global Parameters page appears (see Figure 10-10).

**Figure 10-10 802.11a 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  Enter this command to globally enable CCX radio management:

```
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  Enter these two commands to enable access point customization:

- `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  Enter this command to enable or disable location calibration for a particular client:

```
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  Enter this command to save your settings:

```
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 clients configured for location calibration, enter this command:
   ```
   show client location-calibration summary
   ```

4. To see the RSSI reported for both antennas on each access point that heard the client, enter this command:
   ```
   show client detail client_mac
   ```

Use these commands to obtain radio management debug information for the controller.

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. To debug the output for forwarded probes and their included RSSI for both antennas, enter this command:
   ```
   debug dot11 load-balancing
   ```