APPENDIX A

Radio Resource Management

The operating system security solution uses the radio resource management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them.

Radio Resource Management (RRM) is built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment.

RRM Dashboard

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 presences of voice traffic (in the last 100 ms), the access points defer off-channel measurements and do not change channels.

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.

Cisco WCS provides a snapshot of Radio Resource Management (RRM) statistics to help identify trouble spots and possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (access point performance, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

Note The RRM dashboard information is only available for CAPWAP access points.

Channel Change Notifications

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 cafe affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the cafe 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 difference access point far from the cafe, 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 Mb/s. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

Notifications are sent to the WCS RRM dashboard when a channel change occurs. Channel changes depend on the dynamic channel assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is *auto*, channel assignment is periodically updated for all CAPWAP access

points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based upon request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

DCA supports 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.) You can choose between DCA working at 20 or 40 MHz.

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

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

The controller dynamically controls access point transmit power based on real0time 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 algorithm only reduces an access point's power. However, the coverage hole algorithm 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.

Notifications are sent to the WCS RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs, and each switch optimizes only its own CAPWAP access point parameters. When the grouping is on, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping on, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

The RRM dashboard is accessed by choosing **Monitor > RRM**.

The dashboard is made up of the following parts:

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
- The Channel Change shows all events complete with causes.
- The Configuration Mismatch portion shows comparisons between the leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a screen with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups currently managed by WCS.
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- Percent of APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the present maximum power of the access point.

Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- Channel Change APs—Each event for channel change includes the MAC address of the CAPWAP access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole Events APs—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n CAPWAP access points which are operating at maximum power to accommodate coverage holes and events. The count is split over a 24-hour and 7-day period.

Note This maximum power portion shows the values from the last 24 hours and is poll driven. The power is polled every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n CAPWAP access points which have been operating at maximum power.

Note This maximum power portion shows the value from the last 24 hours and is only event driven.

Configuring Controllers

Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n)

To configure an 802.11a/n or 802.11b/g/n RRM threshold controller, follow these steps.

Step 1 Choose **Configure > Controller**.

Step 2 Click the **IP address** of the appropriate controller to open the **Controller Properties** page.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 4 Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

Note When the Coverage Thresholds Min SNR Level (dB) parameter is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) parameter provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

Step 5 Click **Save**.

Configuring 40-MHz Channel Bonding

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA channels for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM DCA**. The 802.11a/n RRM DCA window appears.

Note You can also configure the channel width on the access point page by choosing **Configure > Access Points** and clicking the **802.11a/n** link in the Radio column. The Current RF Channel Assignment. is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

Step 4 From the Channel Width drop-down menu, choose **20 MHz** or **40 MHz**.

Note Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules which may negatively impact the 20-MHz devices.

Note To view the channel width for an access point's radio, go to **Monitor > Access Points > <name> > Interfaces** tab. You can also view the channel width and antenna selections by choosing **Configure > Access Points** and clicking on the desired radio in the Radio column.

Step 5 Choose the check box(es) for the applicable DCA channel(s). The selected channels are listed in the **Selected DCA channels** text box.

Step 6 Click **Save**.

Configuring Controller Templates

Configuring an RRM Threshold Template for 802.11a/n or 802.11b/g/n

To add a new 802.11a/n or 802.11b/g/n RRM threshold template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click to select a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Thresholds Template appears and the number of controllers the template is applied to automatically populates.

Step 4 Enter the minimum number of failed clients that are currently associated with the controller.

Step 5 Enter the desired coverage level. When the measured coverage drops by the percentage configured in the coverage exception level, a coverage hole is generated.

Step 6 The Signal Strength (dBm) parameter shows the target range of coverage thresholds.

Step 7 Enter the maximum number of clients currently associated with the controller.

Step 8 At the RF Utilization parameter, enter the percentage of threshold for either 802.11a/n or 802.11b/g/n.

Step 9 Enter an interference threshold.

Step 10 Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to WCS.

Step 11 Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Step 12 At the Channel List drop-down menu in the Noise/Interference/Rogue Monitoring Channels section, choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Step 13 Click **Save**.

Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n)

To add an 802.11a/n or 802.11b/g/n RRM interval template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a template name from the Template Name column.

The 802.11a/n or 802.11b/g/n RRM Threshold Template appears and the number of controllers the template is applied to automatically populates.

Step 4 Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point. The default is 300 seconds.

Step 6 Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.

Step 7 Enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 8 Click **Save**.