Monitoring Wireless Technologies

This chapter contains the following sections:

Monitoring Radio Resource Management

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points to automatically discover rogue access points.

RRM, built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

Prime Infrastructure would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into Prime Infrastructure events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

RRM statistics help to identify trouble spots and provide possible reasons for channel or power-level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on event groupings. The event groupings may include the following:

- Worst performing access points
- Configuration mismatch between controllers in the same RF group
- Coverage holes that were detected by access points based on threshold
- Precoverage holes that were detected by controllers
- Ratios of access points operating at maximum power

Note RRM dashboard information is available only for lightweight access points.

Channel Change Notifications

Notifications are sent to the Prime Infrastructure 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 lightweight access points that permit this operation. When the mode is set to on demand, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global defaults.

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

Transmission Power Change Notifications

Notifications are sent to the Prime Infrastructure 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 three modes: Automatic, Off, and Leader. When grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With automatic grouping, 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.)

RRM Dashboard

The RRM dashboard is available at **Monitor > Wireless Technologies > Radio Resource Management**.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups. To get the latest number of RF Groups, run the configuration synchronization background task.
- 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.
  - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
  - WiFi Interference

  - Load
  - Radar
  - Noise
  - Persistent Non-WiFi Interference
  - Major Air Quality Event
  - Other
- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between 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 page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- 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 (derived from all of the controllers which are currently managed by Prime Infrastructure).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- 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 preset value.

  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 with channel changes—Each event for channel change includes the MAC address of the lightweight 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 - APs reporting coverage holes—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

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

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

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

Monitoring Interferers

In the **Monitor > Wireless Technologies > Interferers** page, you can monitor interference devices detected by CleanAir-enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

Table 15-1 lists the menu paths to follow to monitor interferers.

Table 15-1 Menu Paths to Monitor Interferers

To See...	Go To...
AP-detected interferers	**Monitor > Wireless Technologies > Interferers**
AP-detected interferer details	**Monitor > Wireless Technologies > Interferers** > *Interferer ID*
AP-detected interferer details location history	**Monitor > Wireless Technologies > Interferers** > *Interferer ID*, then choose **Select a command** > **Location History** and click **Go**

Related topics

- Field Reference for AP-detected interferers
- Field Reference for AP-detected interferer details
- Field Reference for AP-detected interferer details location history

Configuring the Search Results Display

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. To edit the columns in the AP Detected Interferers page, follow these steps:

Step 1 Choose **Monitor > Wireless Technologies > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring RFID Tags

The **Monitor > Wireless Technologies > RFID Tags** page allows you to monitor tag status and location on Prime Infrastructure maps as well as review tag details.

This page is only available in the Location version of Prime Infrastructure.

This section provides information on the tags detected by the location appliance.

The Tag Summary page is available at **Monitor > Wireless Technologies > RFID Tags**.

Searching RFID Tags

Use the Prime Infrastructure Advanced Search feature to find specific tags or all tags.

To search for tags:

Step 1 Click **Advanced Search**.

Step 2 From the Search Category drop-down list, choose **Tags**.

Step 3 Enter the required information. Note that search fields sometimes change, depending on the category chosen.

Step 4 Click **Go**.

Checking RFID Tag Search Results

To check the search results, click the MAC address of a tag location on a search results page.

Note the following:

- The Tag Vendor option does not appear when Asset Name, Asset Category, Asset Group, or MAC Address is the search criterion.
- Only vendor tags that support telemetry appear.
- The Telemetry data option appears only when MSE (select for location servers), Floor Area, or Outdoor Area is selected as the “Search for tags by” option.
- Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.
- Asset Information, Statistics, Location, and Location Notification details are displayed.
- Only CCX v1 compliant tags are displayed for emergency data.

Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the MAC address, asset details, vendor name, mobility services engine, controller, battery status, and map location.

Monitoring Media Streams

To monitor the media streams configurations, follow these steps:

Step 1 Choose **Monitor > Wireless Technologies > Media Streams**. The Media Streams page appears showing the list of media streams configured across controllers.

The Media Streams page contains a table with the following columns:

- Stream Name—Media Stream name.
- Start IP—Starting IP address of the media stream for which the multicast direct feature is enabled.
- End IP—Ending IP address of the media stream for which the multicast direct feature is enabled.
- State—Operational state of the media stream.
- Max Bandwidth—Indicates the maximum bandwidth that is assigned to the media stream.
- Priority—Indicates the priority bit set in the media stream. The priority can be any number from 1 to 8. A lower value indicates a higher priority. For example, a priority of 1 is highest and a value of 8 is the lowest.
- Violation—Indicates the action to performed in case of a violation. The possible values are as follows:
  - Drop—Indicates that a stream is dropped on periodic revaluation.
  - Best Effort—Indicates that a stream is demoted to best-effort class on periodic reevaluations.
- Policy—Indicates the media stream policy. The possible values are Admit or Deny.
- Controllers—Indicates the number of controllers that use the specified media stream.
- Clients—Indicates the number of clients that use the specified media stream.

Step 2 To view the media stream details, click a media stream name in the Stream column. The Media Streams page appears.

The Media Streams page displays the following group boxes:

- Media Stream Details—Displays the media stream configuration information. This includes the Name, Start Address, End Address, Maximum Bandwidth, Operational Status, Average Packet Size, RRC Updates, Priority, and Violation.
- Statistics—Displays the number of controllers and number of clients that use the selected media stream. Click the controller count to access the list of controllers that use the selected media stream.
- Error—Displays the error, Worst AP, and corresponding floor map for that AP.
- Client Counts—Displays the number of clients for each period.
- Failed Client Counts—Displays the number of clients that failed for each period.

The client information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all the configuration details for the device and network. After successfully joining the wireless controller, the access point can be discovered and managed by Prime Infrastructure. Until the access point successfully joins a wireless controller the access point cannot be managed by Prime Infrastructure and does not contain the proper configuration settings to allow client access.

Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller and lists corrective actions.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included in the page. This includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason if known.

To troubleshoot unjoined access points, do the following:

Step 1 Choose **Monitor > Wireless Technologies > Unjoined Access Points**. The Unjoined APs page appears containing a list of access points that have not been able to join a wireless controller.

Step 2 Select the access point that you wish to diagnose, then click **Troubleshoot**. An analysis is run on the access point to determine the reason why the access point was not able to join a wireless controller. After performing the analysis, the Unjoined APs page displays the results.

Step 3 If the access point has tried to join multiple wireless controllers and has been unsuccessful, the controllers are listed in the left pane. Select a controller.

Step 4 In the middle pane, you can view what the problem is. It will also list error messages and controller log information.

Step 5 In the right pane, recommendations for solving the problems are listed. Perform the recommended action.

Step 6 If you need to further diagnose a problem, you can run RTTS through the Unjoined AP page. This allows you to see the debug messages from all the wireless controllers that the access point tried to join at one time.

To run RTTS, click the RTTS icon () located to the right of the table. The debug messages appear in the table. You can then examine the messages to see if you can determine a cause for the access point not being able to join the controllers.

Monitoring Chokepoints

Chokepoints are low-frequency transmitting devices. When a tag passes within range of a placed chokepoint, the low-frequency field awakens the tag, which, in turn, sends a message over the Cisco Unified Wireless Network that includes the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room-level accuracy (ranging from few inches to 2 feet, depending on the vendor).

Chokepoints are installed and configured as recommended by the chokepoint vendor. After the chokepoint is installed and operational, it can be entered into the location database and plotted on a Prime Infrastructure map.

Related Topic

- Field Reference for Chokepoints Page

Adding a Chokepoint to the Prime Infrastructure Database

To add a chokepoint to the Prime Infrastructure database:

Step 1 Choose **Monitor > Wireless Technologies > Chokepoints**.

Step 2 From the Select a command drop-down list, choose **Add Chokepoint**.

Step 3 Click **Go**.

Step 4 Enter the MAC address and name for the chokepoint.

Step 5 Specify either an entry or exit chokepoint.

Step 6 Enter the coverage range for the chokepoint.

Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click **Save**.

After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add a chokepoint to a map:

Step 1 Choose **Maps > Wireless Maps > Site Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4 Click **Go**.

The Add Chokepoints summary page lists all recently added chokepoints that are in the database but not yet mapped.

Step 5 Select the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left corner. You are now ready to place the chokepoint on the map.

Step 7 Click the chokepoint icon and drag it to the proper location.

The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

The newly created chokepoint icon might or might not appear on the map, depending on the display settings for that floor. The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you hover your mouse cursor over its map icon.

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

Step 10 Synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from the Prime Infrastructure Database

To remove a chokepoint from the Prime Infrastructure database:

Step 1 Choose **Monitor > Wireless Technologies > Chokepoints**.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Removing a Chokepoint from a Prime Infrastructure Map

To remove a chokepoint from a Prime Infrastructure map:

Step 1 Choose **Maps > Wireless Maps > Site Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Editing a Chokepoint

To edit a chokepoint in the Prime Infrastructure database and the appropriate map:

Step 1 Choose **Monitor > Wireless Technologies > Chokepoints**.

Step 2 In the MAC Address column, click the chokepoint that you want to edit.

Step 3 Edit the parameters that you want to change.

The chokepoint range is product-specific and is supplied by the chokepoint vendor.

Step 4 Click **Save**.

Monitoring WiFi TDOA Receivers

The WiFi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset.

Enhancing Tag Location Reporting with WiFi TDOA Receivers

TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Note

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network. See Adding MSEs to Prime Infrastructure.
2. Add the TDOA receiver to Prime Infrastructure database and map. See Adding WiFi TDOA Receivers to Prime Infrastructure and Maps.
3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines. See Synchronizing Prime Infrastructure and MSE.
5. Set up the TDOA receiver using the AeroScout System Manager. See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide for configuration details at the following URL:
http://support.aeroscout.com.

Adding WiFi TDOA Receivers to Prime Infrastructure and Maps

After the WiFi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on a Prime Infrastructure map.

After adding TDOA receivers to Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than Prime Infrastructure.

For more details on configuration options, see the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure database and the appropriate map:

Step 1 Choose **Monitor > Wireless Technologies > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name, and static IP address of the TDOA receiver.

Step 5 Click **Save** to save the TDOA receiver entry to the database.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 Choose **Maps > Wireless Maps > Site Maps**.

Step 7 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9 Click **Go**.

The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10 Select the check box next to each TDOA receiver to add it to the map.

Step 11 Click **OK**.

A map appears with a TDOA receiver icon located in the top-left corner. You are now ready to place the TDOA receiver on the map.

Step 12 Click the TDOA receiver icon and drag it to the proper location on the floor map.

Step 13 Click **Save**.

The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 14.

Step 14 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15 Select the **WiFi TDOA Receivers** check box.

When you hover your mouse cursor over a TDOA receiver on a map, configuration details appear for that receiver.

Step 16 Click **X** to close the Layers page.

Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

Step 17 Download the partner engine software to the mobility services engine.