Monitor Wireless Networks

- What is Radio Resource Management (RRM), on page 1
- RRM Notifications Sent to Prime Infrastructure, on page 2
- Use the RRM Dashboard to Monitor APs, on page 2
- View AP Interferers, on page 4
- View RFID Tagged APs, on page 5
- Monitor Wireless Media Streams, on page 6
- Troubleshoot Unjoined APs, on page 6
- Identify Low-Frequency Transmitting AP Devices (Chokepoints), on page 7
- Add a WiFi TDOA Receiver to MSE, on page 10
- Add WiFi TDOA Receivers to Cisco Prime Infrastructure and Maps, on page 10

What is Radio Resource Management (RRM)

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.

RRM Notifications Sent to Prime Infrastructure

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.

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.

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.)

Use the RRM Dashboard to Monitor APs

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.

View AP 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 1: Menu Paths to Monitor Interferers

To See...	Go To...
AP-detected interferers	**Monitor > Wireless Technologies > Interferers** **Note** This page does not display Interferers if using CMX.
AP-detected interferer details	**Monitor** > **Wireless Technologies** > **Interferers** > **Interferer ID**
AP-detected interferer details location history	**Monitor** > **Wireless Technologies** > **Interferers** > **Interferer ID**, then choose S**Location History**, and click **Go**.

Edit the AP Detected Interferers Page

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:

SUMMARY STEPS

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

6. Click **Reset** to restore the default view.
7. Click **Submit** to confirm the changes.

DETAILED 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.

View RFID Tagged APs

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**.

Search for RFID Tags

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

To search for tags:

SUMMARY STEPS

1. Click **Advanced Search**.
2. From the Search Category drop-down list, choose **Tags**.
3. Enter the required information. Note that search fields sometimes change, depending on the category chosen.
4. Click **Go**.

DETAILED STEPS

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**.

Check 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.

View 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.

Monitor Wireless 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.

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

Troubleshoot Unjoined APs

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.

Identify Low-Frequency Transmitting AP Devices (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.

Add AP Chokepoints to Prime Infrastructure

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.

Note Prime Infrastructure does not support Embedded Wireless Controller on an Access Point (EWC). It is only supported by Cisco DNA Centre.

Remove AP Chokepoints from Prime Infrastructure

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**.

Step 4 Click **Go**.

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

Remove Chokepoints from Prime Infrastructure Maps

To remove a chokepoint from a Prime Infrastructure map:

SUMMARY STEPS

1. Choose **Maps > Wireless Maps > Site Maps**.
2. In the Maps page, click the link that corresponds to the floor location of the chokepoint.
3. From the Select a command drop-down list, choose **Remove Chokepoints.**
4. Click **Go**.
5. Click **OK** to confirm the deletion.

DETAILED STEPS

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.

Edit AP Chokepoints

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**.

Enhance 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.

Note 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 Add MSEs to Cisco Prime Infrastructure.
2. Add the TDOA receiver to Prime Infrastructure database and map. See Add WiFi TDOA Receivers to Cisco Prime Infrastructure and Maps, on page 10.
3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines. See Cisco Prime Infrastructure Data That is Synchronized With 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

Add a WiFi TDOA Receiver to MSE

After the Wi-Fi 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 an Prime Infrastructure map.

After adding TDOA receivers to the Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than the 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:XREF http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure database and appropriate map, follow these steps:

Step 1 Choose **Configuration** > **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**, then click **Go**.

Step 3 Enter the MAC address, name and static IP address of the TDOA receiver.

Step 4 Click **OK** to save the TDOA receiver entry to the database.

After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map.

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

Add WiFi TDOA Receivers to Cisco 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.