CHAPTER 17

Working with Wireless Operational Tools

The Wireless Operational Tools menu provides access to the Guest User Controller Templates, Voice Audit, Voice Diagnostic, Location Accuracy Tool, Configuration Audit Summary, Migration Analysis, Radio Resource Management (RRM), RFID Tags, Chokepoints, Interferers, Spectrum Experts, and WiFi TDOA Receivers features of the Cisco Prime Infrastructure. This chapter contains the following sections:

Configuring Guest User Templates

This page allows you to add a guest user template or make modifications to an existing guest user template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. See theManaging Guest User Accounts, page 28-4 for further information on guest access.

Step 1 Choose **Operate > Operational Tools > Wireless > Guest User**. The Guest Users Controller Templates page appears.

Note To reduce clutter, Prime Infrastructure does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

Step 2 If you want to add a new template, choose **Add Guest User** from the Select a command drop-down list, and click **Go**. The New Controller Template page appears.

Note You can also modify an existing template by clicking the template name link.

Step 3 In the New Controller Template page, complete the fields as described in Table 31-68 and Table 31-69.

Step 4 Click **Save**.

Running Voice Audits

Prime Infrastructure provides voice auditing mechanism to check the controller configuration and to ensure that any deviations from the deployment guidelines are highlighted as an Audit Violation.

To access the Voice Audit feature, choose **Operate > Operational Tools > Wireless > Voice Audit**. The Voice Audit Report page appears. For information about the tabs and fields on this page, see Table 31-70.

This section contains the following topic:

- Running Voice Audits on Controllers, page 17-2

Running Voice Audits on Controllers

To run the voice audit, you must first choose the controller(s) on which to run the voice audit, and then indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.

The Controllers tab allows you to choose the controller(s) on which to run the voice audit and the Rules tab allows you to indicate the applicable rules for the voice audit.

Note You can run the voice audit on a maximum of 50 controllers in a single operation.

To run the voice audit:

Step 1 Choose **Operate > Operational Tools > Wireless > Voice Audit**.

Step 2 Click the **Controllers** tab, and complete the fields as described in

Step 3 Click the **Rules** tab to determine the rules for this voice audit.

Step 4 In the VoWLAN SSID field, type the applicable VoWLAN SSID. For information about the Rules and Rule Details, see Table 31-71.

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Step 5 When the rules are configured for this voice audit, click **Save** to save the current configuration or **Save and Run** to save the configuration and run the report.

Step 6 Click the **Report** tab to view the Report results. See Table 31-72for more information.

Running Voice Diagnostic

The Voice diagnostic tool is an interactive tool to diagnose the voice calls in real time. This tool reports call control related errors, roaming history of the clients and the total active calls accepted and rejected by an associated AP. This tool enables you to start or stop the voice diagnostic.

The Voice diagnostic test is provisioned for multiple controllers, that is if the AP is associated to more than one controller during roaming, the Voice diagnostics tests all the associated controllers. Prime Infrastructure supports testing on controllers whose APs are placed on +/- 3 floors. For example, Prime Infrastructure map has floors 1 to 4 and all APs are associated to controllers (wlc1, wlc2, wlc3, wlc4) and are placed on the Prime Infrastructure map, if a client is associated on any AP with WLC1 on first floor and if voice diagnostic test is started for this client, test will also be provisioned on wlc2 to wlc3 also). This is done for roaming reason.

The Voice diagnostic page lists the prior test runs, if any. For information about the fields on this page, see Table 31-73.

You can either start a new test or view the existing test results or delete a test from the Select a command from the drop-down list.

Note To support roaming, the tool figures out controllers in the same building as of client's associated AP building and adds to all controller's watchlist. The tool looks for controllers in +/-5 floors from client's current association A's location to configure on controllers. Configuration on controller's watchlist is done for 10 minutes. After 10 minutes controller will remove the entry from the watchlist.

This section contains the following topic:

Starting the Voice Diagnostic Test

To start a Voice Diagnostic test:

Step 1 Click **Operate > Operational Tools > Wireless > Voice Diagnostics**.

Step 2 From the Select a command drop-down list, click the New test and click Go. It takes you to the configuration page.

Note On this page, you can configure maximum of two clients for voice call diagnosis. Both clients can be on the same call or can be in a different call.

Step 3 Enter the Test name and the time duration to monitor the voice call. You can do a voice diagnosis test for 10, 20, 30, 40, 50 or 60 minutes. 10 minutes is the default duration selected by Prime Infrastructure.

Step 4 Enter the MAC address of the device for which you want to do the voice diagnostic test.

Step 5 Select the device type. It could be either a cisco based phone or custom phones. If it is a custom phone you have to enter the RSSI range for the custom phone. For Cisco phones the RSSI range is preselected.

Step 6 Click StartTest to start the test or if the test is completed you can restart the test.

Note If the test is not completed the state is Running and if test is completed then the state is Completed. To stop the test in between, you can use the Stop button, the state is then stopped.

For information about the details displayed on the Voice Diagnostic Test Report page, see Table 31-74.

Configuring the Location Accuracy Tools

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy Tools.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy Tools enable you to run either of the following tests:

There are two ways to test location accuracy:

- **Scheduled Accuracy Testing**—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already pre-positioned so that the test can be run on a regularly scheduled basis.
- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

This section contains the following topics:

Enabling the Location Accuracy Tool

Note You must enable the **Advanced Debug** option in Prime Infrastructure to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy Tool does not appear as an option on the Operate > Operational Tools > Wireless menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in Prime Infrastructure:

Step 1 In Prime Infrastructure, choose **Operate > Maps**.

Step 2 Choose **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 In the page that appears, select the **Enabled** check box to enable the Advanced Debug Mode. Click **OK**.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

You can now run location accuracy tests on the mobility services engine using the Location Accuracy Tool.

Use the Select a command drop-down list to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.

Note

- You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either **Download Logs** or **Download Logs for Last Run**. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test:

Step 1 Choose **Operate > Operational Tools > Wireless > Location Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a Test Name.

Step 4 Choose the **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the begin and end time of the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.

Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 9 Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.

Note If you choose the e-mail option, an SMTP Mail Server must first be defined for the target e-mail address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.

Step 10 Click **Position Testpoints**. The floor map appears with a list of all clients, tags, and interferers on that floor with their MAC addresses.

Step 11 Select the check box next to each client, tag, and interferer for which you want to check the location accuracy.

When you select a MAC address check box, two icons appear on the map. One icon represents the actual location and the other represents the reported location.

Note To enter a MAC address for a client or tag or interferer that is not listed, select the **Add New MAC** check box, enter the MAC address, and click **Go**. An icon for the element appears on the map. If the newly added element is on the location server but on a different floor, the icon is displayed in the left-most corner (0,0 position).

Step 12 If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. Only the actual location icon can be dragged.

Step 13 Click **Save** when all elements are positioned. A dialog box appears confirming successful accuracy testing.

Step 14 Click **OK** to close the confirmation dialog box. You are returned to the Accuracy Tests summary page.

Note The accuracy test status is displayed as Scheduled when the test is about to execute. A status of Running is displayed when the test is in process and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 15 To view the results of the location accuracy test, click the test name and then click the **Results** tab in the page that appears.

Step 16 In the Results page, click the **Download** link under the Saved Report heading to view the report.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

Using On-demand Accuracy Testing to Test Location Accuracy

An On demand Accuracy Test is run when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

To run an On-demand Accuracy Test:

Step 1 Choose **Operate > Operational Tools > Wireless > Location Accuracy Tool**.

Step 2 From the Select a command drop-down list, choose **New On demand Accuracy Test**.

Step 3 Enter a Test Name.

Step 4 Choose **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the Destination point for the test results. Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.

Step 9 Click **Position Testpoints**. The floor map appears with a red crosshair at the (0,0) coordinate.

Step 10 To test the location accuracy and RSSI of a particular location, select either client or tag or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client or tag or interferer) displays in a drop-down list to its right.

Step 11 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 12 From the Zoom percentage drop-down list, choose the zoom percentage for the map.

The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.

Step 13 Click **Start** to begin collection of accuracy data.

Step 14 Click **Stop** to finish collection. You should allow the test to run for at least two minutes before clicking Stop.

Step 15 Repeat Step 11 to Step 14 for each testpoint that you want to plot on the map.

Step 16 Click **Analyze Results** when you are finished mapping the testpoints.

Step 17 Click the **Results** tab in the page that appears.

The On-demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph

Configuring Audit Summary

Choose **Operate > Operational Tools > Wireless > Configuration Audit** to launch the Config Audit Summary page.

This page provides a summary of the following:

- Total Enforced Config Groups—Identifies the count of config group templates, which are configured for Background Audit and are enforcement enabled.

  Click the link to launch the Config Group page to view config groups with Enforce Configuration enabled.

- Total Mismatched Controllers—Identifies the number of mismatched controllers. Mismatched controllers indicate that there were configuration differences found between Prime Infrastructure and the controller during the last audit.

  Click the link to launch the controller list sorted in the mismatched audit status column. Click an item in the Audit Status column to view the audit report for this controller.

- Total Config Audit Alarms—Identifies the number of alarms generated when audit discrepancies are enforced on config groups.

  Click the link to view all config audit alarm details.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Most recent 5 config audit alarms—Lists the most recent configuration audit alarms including the object name, event type, date, and time for the audit alarm.

Click **View All** to view the applicable Alarm page that includes all configuration audit alarms.

Configuring Migration Analysis

Choose **Operate > Operational Tools > Wireless > Migration Analysis** to launch the Migration Analysis Summary page.

Note You can also access the migration analysis summary by choosing **Design > Wireless Configuration > Autonomous AP Migration Templates** and choosing **View Migration Analysis Summary** from the Select a command drop-down list.

The autonomous access points are eligible for migration only if all the criteria has a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version—Conversion is supported only from 12.3(7)JA releases excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only

Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

This section contains the following topics:

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. In the Migration Analysis page, you can select the access point with the software version listed as failed and choose **Upgrade Firmware (Manual or Automatic)** from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

Prime Infrastructure uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in Prime Infrastructure. The default images per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional page with TFTP server IP, file path, and file path name appears. The final page is the Report page.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, choose **Change Station Role to Root Mode** from the Select a command drop-down list to change the mode.

Running Migration Analysis

Choose **Run Migration Analysis** from the Select a command drop-down list of the Migration Analysis Summary page. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Viewing the Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down list of the Migration Analysis Summary page to generate a report. The report includes the following:

- Access point address
- Status
- Timestamp
- Access point logs

Viewing a Firmware Upgrade Report

Choose **View Firmware Upgrade Report** from the Select a command drop-down list to view a current report of the upgrade status for the selected access point.

The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the firmware upgrade.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

See the "Upgrading Autonomous Access Points" section on page 17-9 for more information.

Viewing a Role Change Report

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role.

To view a report of these role changes, choose **View Role Change Report** from the Select a command drop-down list. The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the role change.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Monitoring Radio Resource Management (RRM)

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

Radio Resource Management (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.

Radio Resource Management (RRM) statistics helps to identify trouble spots and provides 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 (worst performing access points, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, pre-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 lightweight access points.

This section contains the following topics:

Channel Change Notifications

Notifications are sent to 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 which 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 default.

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

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

Choose **Operate > Operational Tools > Wireless > Radio Resource Management** to access the RRM dashboard.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups.

Note To get the latest number of RF Groups, you have to run the configuration sync 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 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.

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 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.

Note 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.

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

Monitoring RFID Tags

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

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

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

Choose **Operate > Operational Tools > Wireless > RFID Tags** to access this section. By default, the Tag Summary page is displayed.

This section contains the following topics:

Tag Summary

Choose **Operate > Operational Tools > Wireless > RFID Tags** to access this page.

This page provides information on the number of tags that are detected by MSE. The following fields are displayed in the main data area:

- Device Name—Name of the MSE device.
- Total Tags—Click the number to view tag details. Clicking the number shows the list of tags located by the MSE. Clicking a MAC address shows the tag details pertaining to that MAC address.

Searching Tags

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

To search for tags in Prime Infrastructure:

Step 1 Click **Advanced Search**.

Step 2 Choose **Tags** from the Search Category drop-down list.

Step 3 Identify the applicable tag search fields including:

- **Search By**—Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.

  Note Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

- **Search In**—Choose MSEs or Prime Infrastructure Controllers.
- **Last detected within**—Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
- **Tag Vendor**—Select the check box, and choose **Aeroscout**, **G2**, **PanGo**, or **WhereNet**.
- **Telemetry Tags only**—Select the Telemetry Tags only check box to search tags accordingly.

Step 4 Click **Go**.

Viewing RFID Tag Search Results

Use Prime Infrastructure Advanced Search feature located in the top right of Prime Infrastructure page to search for tags by asset type (name, category and group), by MAC address, by system (controller or location appliance), and by area (floor area and outdoor area).

Note Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

You can further refine your search using the Advanced search fields and save the search criteria for future use. Saved search criteria can be retrieved from the Saved Searches located in the navigation bar. For more information, see Advanced Search and Saved Searches in the Cisco Prime Infrastructure Configuration Guide, Release1.2.

When you click the MAC address of a tag location in a search results page, the following details appear for the tag:

- Tag vendor

Note This option does not appear when Asset Name, Asset Category, Asset Group or MAC Address are the search criteria for tags.

- Controller to which the tag is associated
- Telemetry data (CCX v1 compliant tags only)
  - 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.

Note The Telemetry data option only appears when MSE (select for location servers), Floor Area, or Outdoor Area are selected as the Search for tags by option.

Note Only those vendor tags that support telemetry appear.

- Asset Information (Name, Category, Group)
- Statistics (bytes and packets received)
- Location (Floor, Last Located, MSE, map)
- Location Notification (Absence, Containment, Distance, All)

Note 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.

- Emergency Data (CCX v1 compliant tags only)

Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the following information:

- MAC Address
- Asset Name
- Asset Group
- Asset Category
- Vendor Name

- Mobility Services Engine
- Controller
- Battery Status
- Map Location

Configuring Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including 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 installation is complete and operational, the chokepoint can be entered into the location database and plotted on a Prime Infrastructure map.

This section contains the following topics:

Configuring New Chokepoints

This section contains the following topics:

Adding a Chokepoint to Prime Infrastructure Database

To add a chokepoint to Prime Infrastructure database:

Step 1 Choose **Operate > Operational Tools > Wireless > 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 Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 6 Enter the coverage range for the chokepoint.

Note 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 **OK**.

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

Adding a Chokepoint to an Prime Infrastructure Map

To add the chokepoint to a map:

Step 1 Choose **Operate > 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**.

Note 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 hand corner. You are now ready to place the chokepoint on the map.

Step 7 Left-click the chokepoint icon and drag and place it in the proper location.

Note 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**.

You are returned to the floor map and the added chokepoint appears on the map.

Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

Note 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.

Note MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse 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.

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

Note You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from a Prime Infrastructure Map

To remove an chokepoint from the map:

Step 1 Choose **Operate > Maps**.

Step 2 In the Maps page, choose 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.

Removing a Chokepoint from Prime Infrastructure

To remove a chokepoint from Prime Infrastructure:

Step 1 Choose **Operate > Operational Tools > Wireless > 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.

Editing Current Chokepoints

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

Step 1 Choose **Operate > Operational Tools > Wireless > Chokepoints**. The Configure > Chokepoints page displays the following information for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.

Step 2 Click the chokepoint you want to edit in the MAC Address column.

Step 3 Edit the following parameters, as necessary:

- Name
- Entry/Exit Chokepoint—Click to enable.
- Range—Coverage range for the chokepoint.

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

- Static IP Address

Step 4 Click **Save**.

Monitoring Interferers

The Monitor > Interferers page allows you to monitor interference devices detected by the CleanAir enabled access points.

This section provides information on the interferers detected by the CleanAir enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

This section contains the following topics:

Monitoring AP Detected Interferers

Choose **Operate > Operational Tools > Wireless > Interferers** to view all the interfering devices detected by the CleanAir enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device. Click this link to know more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. A pop-up window appears displaying more details. The categories include the following:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Owen—A microwave oven (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter

  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
  - Video Camera—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted WiFi signals
  - WiFi Invalid Channel—A device using non-standard WiFi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device
  - Radar—A radar device (802.11a/n only)
  - XBox—A Microsoft Xbox (802.11b/g/n only)
  - WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
  - WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
  - WiFi AOCI—A WiFi device with AOCI
  - Unclassified
- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by Prime Infrastructure.
- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

Monitoring AP Detected Interferer Details

Choose **Operate > Operational Tools > Wireless > Interferers >** *Interferer ID* to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.
- Status—The status of the interfering device. Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by Prime Infrastructure.
  - Severity—Displays the severity ranking of the interfering device.
  - Duty Cycle (%)—The duty cycle of interfering device in percentage.

  - Affected Band—Displays the band in which this device is interfering.
  - Affected Channels—Displays the affected channels.
  - Discovered—Displays the time at which it was discovered.
  - Last Updated—The last time the interference was detected.
- Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The mobility server engine on which this interference device was located.
- Clustering Information
  - Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point.
  - Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).
- Details—Displays a short description about the interfering type.

Monitoring AP Detected Interferer Details Location History

Choose **Operate > Operational Tools > Wireless > Interferers >** *Interference Device ID,* then choose **Location History** from the Select a command drop-down list, and click **Go** to view this page.

- Interferer Information—Displays the basic information about the interfering device.
  - Data Collected At—The time stamp at which the data was collected.
  - Type—The type of the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle—The duty cycle (in percentage) of the interfering device.
  - Affected Channels—A comma separated list of the channels affected.
- Interferer Location History—Displays the location history of the interfering devices.
  - Time Stamp
  - Floor
- Clustering Information
  - Clustered By
- Detecting APs
  - AP Name—The access point that detected the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location
  - Location Calculated At—Displays the time stamp at which this information was generated.
  - Floor—Displays location information of the interfering device.
  - A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

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:

Step 1 Choose **Operate > Operational Tools > Wireless > 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.

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose **Operate > Operational Tools > Wireless > Spectrum Experts**. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to Prime Infrastructure. The status appears as reachable or unreachable.

This section contains the following topics:

- Adding a Spectrum Expert, page 17-23
- Spectrum Experts Details, page 17-23

Adding a Spectrum Expert

To add a Spectrum Expert:

Step 1 Choose **Operate > Operational Tools > Wireless > Spectrum Experts**.

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

Note This link only appears when no spectrum experts are added.

Step 3 Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

Note To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to Prime Infrastructure.

Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds providing a real-time look at what is happening on the remote Spectrum Expert and includes the following items:

- Total Interferer Count—As seen by the specific Spectrum Expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferes by category.
- Active Interferer Count Per Channel—Displays the number of interferes grouped by category on different channels.
- AP List—Provides a list of access points detected by the Spectrum Expert that are on channels that have active interferers detected by the Spectrum Expert on those channels.
- Affected Clients List—Provides a list of clients that are currently authenticated/associated to the radio of one of the access points listed in the access point list.

Configuring Wi-Fi TDOA Receivers

This section contains the following topics:

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi 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. 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 a Mobility Services Engine, in the Cisco Prime Infrastructure Configuration Guide, Release 1.2, for details on adding a mobility services engine.

2. Add the TDOA receiver to Prime Infrastructure database and map.

   See Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps for details on adding the TDOA receiver to Prime Infrastructure.

3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines.

   See Synchronizing Services, in the Cisco Prime Infrastructure Configuration Guide, Release 1.2, for details on synchronization.

5. Set up the TDOA receiver using the AeroScout System Manager.

Note 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 Wi-Fi TDOA Receivers to Prime Infrastructure and Maps

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

Note 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 Prime Infrastructure database and appropriate map:

Step 1 Choose **Operate > Operational Tools > Wireless > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Note 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 **OK** to save the TDOA receiver entry to the database.

Note After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map. To do so, continue with Step 6.

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

Step 6 To add the TDOA receiver to a map, choose **Operate > 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**.

Note 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 hand corner. You are now ready to place the TDOA receiver on the map.

Step 12 Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

Note The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

Step 13 Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

Note 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. The TDOA receiver appears on the map.

Note When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.

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

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

Step 17 You can now download the partner engine software to the mobility services engine.