CHAPTER 14

Reports

Cisco NCS reporting is necessary to monitor the system and network health as well as troubleshoot problems. A number of reports can be generated to run on an immediate and scheduled basis. Each report type has a number of user-defined criteria to aid in the defining of the reports. The reports are formatted as a summary, tabular, or combined (tabular and graphical) layout. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on NCS for later download or e-mailed to a specific e-mail address.

The reporting types include the following:

- Current, which provides a snap shot of the data that is not dependent upon time.
- Historical, which retrieves data from the device periodically and stores it in the NCS database
- Trend, which generates a report using aggregated data. Data can be periodically collected based from devices on user-defined intervals, and a schedule can be established for report generation.

With NCS, you also have the ability to export any report that you can view, sort reports into logical groups, and archive for long-term storage.

Note As of NCS 1.0, the size limitations of reports is removed. So, you can view a report of any size with any number of graphs using HTML or saved as CSV/PDF files.

The Reports menu provides access to all NCS reports as well as currently saved and scheduled reports.

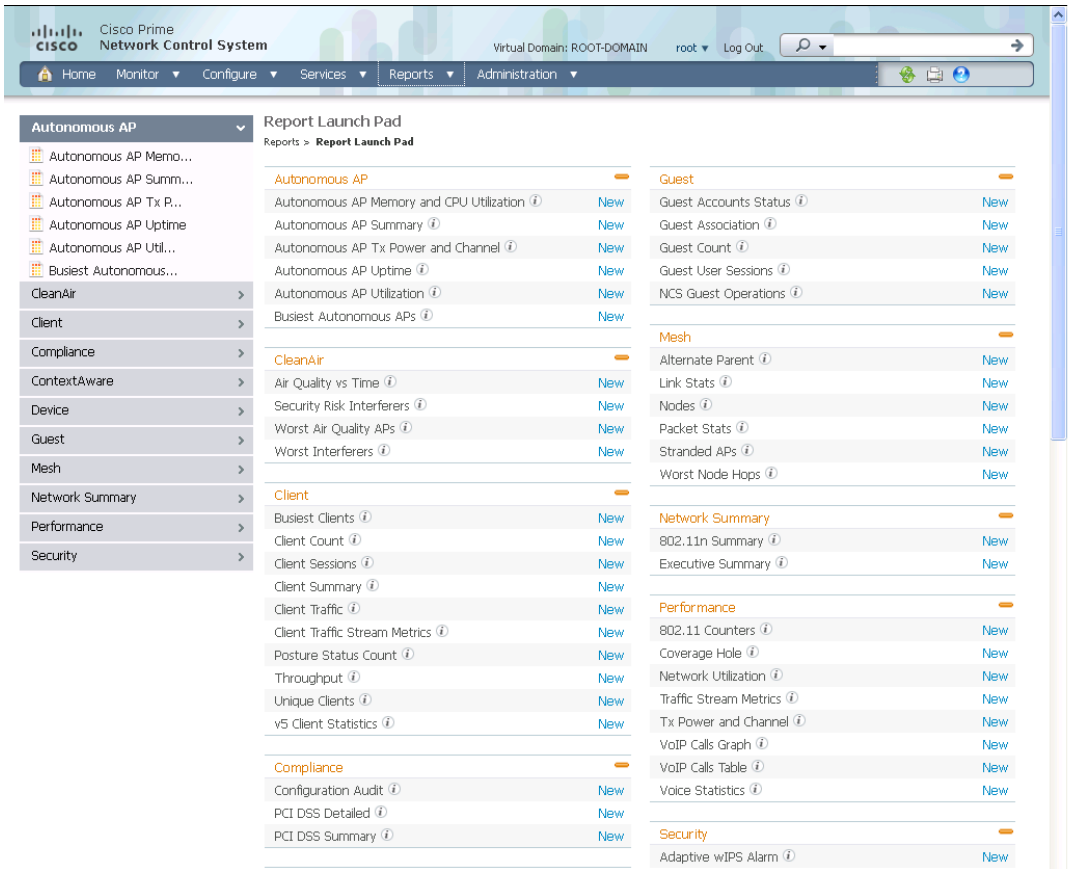
- Report Launch Pad—The hub for all NCS reports. From this page, you can access specific types of reports and create new reports. See the "Report Launch Pad" section on page 14-2 for more information.
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in NCS. In addition, allows you to access and manage on-demand export as well as e-mailed reports. See the "Managing Scheduled Run Results" section on page 14-14 for more information.
- Saved Report Templates—Allows you to access and manage all currently saved report templates in NCS. See the "Managing Saved Report Templates" section on page 14-16 for more information.

Report Launch Pad

The report launch pad provides access to all NCS reports from a single page. From this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs (see Figure 14-1).

Tip Hover your mouse cursor over the tool tip next to the report type to view more report details.

Figure 14-1 Report Launch Pad



This section contains the following topics:

- Mapping Reports in WCS with Reports in NCS, page 14-3
- Creating and Running a New Report, page 14-6
- Managing Current Reports, page 14-13
- Managing Scheduled Run Results, page 14-14
- Managing Saved Report Templates, page 14-16

Mapping Reports in WCS with Reports in NCS

Table 14-1 provides the mapping between the reports in WCS and Reports in NCS. Additionally, the new reports that were added to NCS are also specified.

Table 14-1 Mapping Reports in WCS with Reports in NCS

Reports	In WCS	In NCS
Autonomous AP	-	-
Autonomous AP Memory and CPU Utilization	No	Yes
Autonomous AP Summary	No	Yes
Autonomous AP Tx Power and Channel	No	Yes
Autonomous AP Uptime	No	Yes
Autonomous AP Utilization	No	Yes
Busiest Autonomous APs	No	Yes
CleanAir	-	-
Air Quality vs Time	Yes	Yes
Security Risk Interferers	Yes	Yes
Worst Air Quality APs	Yes	Yes
Worst Interferers	Yes	Yes
Client	-	-
Busiest Clients	Yes	Yes
Client Count	Yes	Yes
Client Sessions	Yes	Yes
Client Summary	Yes	Yes
Client Traffic	Yes	Yes
Client Traffic Stream Metrics	Yes	Yes
Posture Status Count	No	Yes
Throughput	Yes	Yes
Unique Clients	Yes	Yes
v5 Client Statistics	Yes	Yes
Compliance	-	-
Configuration Audit	Yes	Yes
PCI DSS Detailed	Yes	Yes
PCI DSS Summary	Yes	Yes
ContextAware	-	-
Client Location History	Yes	Yes
Client Location Tracking	Yes	Yes

Table 14-1 Mapping Reports in WCS with Reports in NCS (continued)

Reports	In WCS	In NCS
Guest Location Tracking	Yes	Yes
Location Notifications	Yes	Yes
Rogue AP Location Tracking	Yes	Yes
Rogue Client Location Tracking	Yes	Yes
Tag Location History	Yes	Yes
Tag Location Tracking	Yes	Yes
Device	-	-
AP Image Pre-download	Yes	Yes
AP Profile Status	Yes	Yes
AP Summary	Yes	Yes
Busiest APs	Yes	Yes
CPU Utilization	Yes	Yes
Detailed Switch Inventory	No	Yes
Identity Capability	No	Yes
Inventory	No	Yes
Memory Utilization	Yes	Yes
Non-Primary Controller APs	No	Yes
Switch Interface Utilization	No	Yes
Up Time	Yes	Yes
Utilization	Yes	Yes
Guest	-	-
Guest Accounts Status	Yes	Yes
Guest Association	Yes	Yes
Guest Count	Yes	Yes
Guest User Sessions	Yes	Yes
NCS Guest Operations	Yes	Yes
Identity Services Engine	--	--
Posture Detail Assessment	No	Yes
Endpoint Profiler Summary	No	Yes
Top N Endpoint MAC Authentications	No	Yes
Endpoint MAC Authentication Summary	No	Yes
User Authentication Summary	No	Yes
Top N User Authentications	No	Yes
Radius Accounting	No	Yes
Radius Authentication	No	Yes

Table 14-1 Mapping Reports in WCS with Reports in NCS (continued)

Reports	In WCS	In NCS
Mesh	-	-
Alternate Parent	Yes	Yes
Link Stats	Yes	Yes
Nodes	Yes	Yes
Packet Stats	Yes	Yes
Stranded APs	Yes	Yes
Worst Node Hops	Yes	Yes
Network Summary	Yes	Yes
802.11n Summary	Yes	Yes
Executive Summary	Yes	Yes
Performance	-	-
802.11 Counters	Yes	Yes
Coverage Hole	Yes	Yes
Network Utilization	Yes	Yes
Traffic Stream Metrics	Yes	Yes
Tx Power and Channel	Yes	Yes
VoIP Calls Graph	Yes	Yes
VoIP Calls Table	Yes	Yes
Voice Statistics	Yes	Yes
Security	-	-
Adaptive wIPS Alarm	Yes	Yes
Adaptive wIPS Alarm Summary	Yes	Yes
Adaptive wIPS Top 10 AP	Yes	Yes
Adhoc Rogue Count Summary	Yes	Yes
Adhoc Rogues	Yes	Yes
New Rogue AP Count Summary	Yes	Yes
New Rogue APs	Yes	Yes
Rogue AP Count Summary	Yes	Yes
Rogue APs	Yes	Yes
Security Alarm Trending Summary	Yes	Yes

Non Upgradable Reports from WCS to NCS

The following reports cannot be upgraded to NCS 1.0:

- Client Count
- Client Summary

- Client Throughput
- Security Summary
- Adhoc Rogue Count Summary
- Adhoc Rogues
- New Rogue AP Count Summary
- New Rogue APs
- Rogue AP Count Summary
- Rogue APs

Creating and Running a New Report

To create and run a new report, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

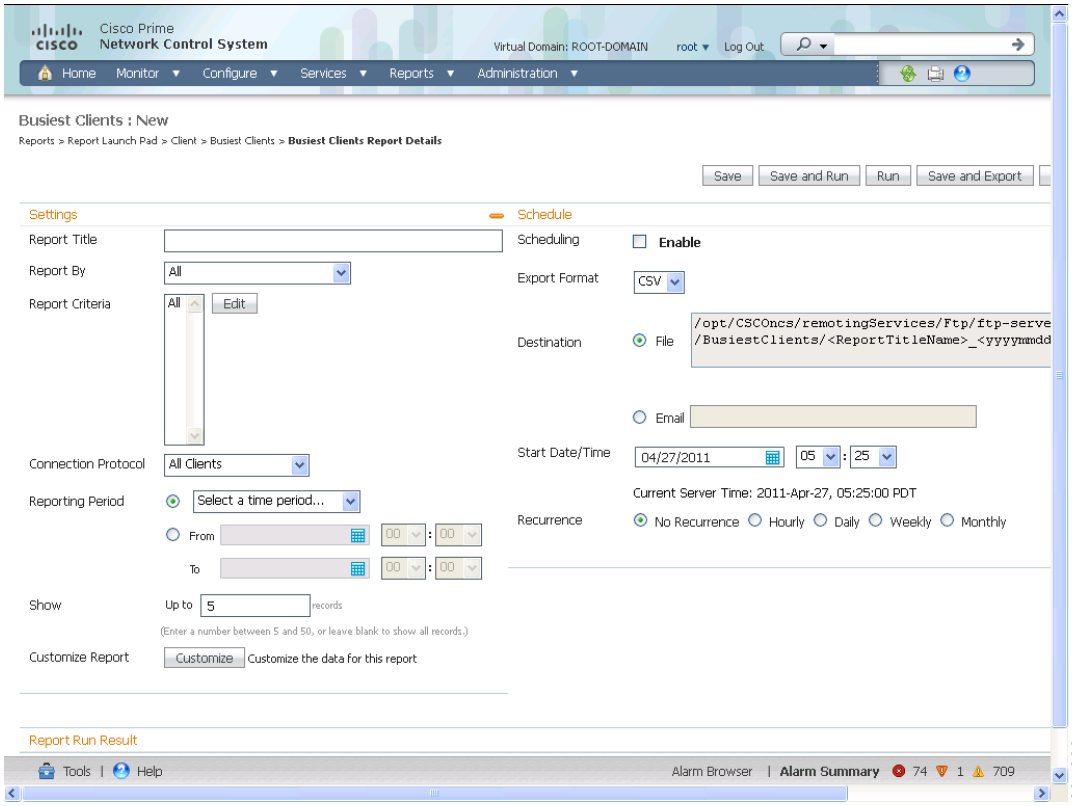
The reports are listed by category in the main section of the page and on the left sidebar menu (see Figure 14-1).

Step 2 Find the appropriate report in the main section of the Report Launch Pad.

Note Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved report templates for that report type.

Step 3 Click **New** to the right of the report. The Report Details page appears (see Figure 14-2).

Figure 14-2 Report Details Page



Step 4 In the Report Details page, enter the following Settings parameters:

Note Certain parameters may or may not appear depending on the report type.

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By—Choose the appropriate Report By category from the drop-down list. The categories differ for each report. See specific report sections for Report By categories for each report.
- Report Criteria—The parameter allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.

Note Click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Communication Protocol—Choose either of these protocols **All Clients, All Wired (802.3), All Wireless (802.11), 802.11a/n**, **802.11b/g/n**, **802.11a, 802.11b, 802.11g, 802.11n (5 GHz)**, or **802.11n (2.4 GHz)**.
- Report Period
  - Last—Select the **Last** radio button and choose the period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Step 5 If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.

- Enable Schedule—Select the check box to run the report on the set schedule.
- Export Format—Choose your format for exported files (CSV or PDF).
- Destination—Choose your destination type (File or Email). Enter the applicable file location or the e-mail address.

Note The default file locations for CSV and PDF files are as follows:

/ncs-ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv
/ncs-ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

Note To set the mail server setup for e-mails, choose **Administration > Settings**, then choose **Mail Server** from the left side-bar menu to open the Mail Server Configuration page. Enter the SMTP and other required information.

- Start Date/Time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report will begin running on this data and at this time.

Note The time referred here is the NCS server time and not the local time of the browser.

- Recurrence—Enter the frequency of this report.
  - No Recurrence—The report runs only once (at the time indicated for the Start Date/Time).
  - Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box.
  - Daily—The report runs on the interval indicated by the number of days you enter in the Every text box.
  - Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.

The Create Custom Report page allows you to customize the report results. Table 14-2 specifies which reports are customizable, which have multiple sub-reports, and which report views are available. In future releases, all reports will be customizable.

Table 14-2 Report Customization

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Autonomous AP Memory and CPU Utilization	No	No	Graphical	No
Autonomous AP Summary	Yes	No	Tabular	No
Autonomous AP Tx Power and Channel	No	Yes	Graphical	No
Autonomous AP Uptime	Yes	No	Tabular	No
Autonomous AP Utilization	No	No	Graphical	No
Busiest Autonomous APs	Yes	No	Tabular	No
Air Quality vs Time	Yes	No	Tabular	No
Security Risk Interferers	Yes	No	Tabular	No
Worst Air Quality APs	Yes	No	Tabular	No
Worst Interferers	Yes	No	Tabular	No
Busiest Clients	Yes	No	Tabular	No
Client Count	No	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic	No	No	Graphical	No
Client Traffic Stream Metrics	Yes	No	Tabular[1]	No
Posture Status Count	No	No	Graphical	No
Throughput	No	No	Tabular	No
Unique Clients	Yes	No	Tabular	No
v5 Client Statistics	No	No	Tabular	No
Configuration Audit	Yes	No	Tabular	No
PCI DSS Detailed	Yes	No	Tabular	No
PCI DSS Summary	No	No	Graphical	No
Client Location History	Yes	No	Tabular	No
Client Location Tracking	Yes	No	Tabular	No
Guest Location Tracking	Yes	No	Tabular	No

Table 14-2 Report Customization (continued)

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Location Notifications	Yes	No	Tabular	No
Rogue AP Location Tracking	Yes	No	Tabular	No
Rogue Client Location Tracking	Yes	No	Tabular	No
Tag Location History	Yes	No	Tabular	No
Tag Location Tracking	Yes	No	Tabular	No
AP Image Pre-download				
AP Profile Status	Yes	No	Tabular	No
AP Summary				
Device Summary	Yes	No	Tabular	No
Busiest APs	Yes	No	Tabular	No
CPU Utilization	No	No	Graphical	No
Detailed Switch Inventory	Yes	Yes	Tabular	No
Identity Capability	No	No	Various	No
Inventory - Combined Inventory	Yes	Yes	Various[2]	Yes
Inventory - APs	Yes	Yes	Various	Yes
Inventory - Controllers	Yes	Yes	Various	Yes
Inventory - MSEs	Yes	Yes	Various	Yes
Up Time	Yes	No	Tabular	No
Utilization - Controllers	No	No	Graphical	No
Utilization - MSEs	No	No	Graphical	No
Utilization - Radios	No	No	Graphical	No
Guest Account Status	Yes	No	Tabular	No
Guest Association	Yes	No	Tabular	No
Guest Count	No	No	Tabular	No
Guest User Sessions	Yes	No	Tabular	No
NCS Guest Operations	Yes	No	Tabular	No
Alternate Parent	Yes	No	Tabular	No
Link Stats - Link Stats	Yes	No	Tabular	No
Link Stats - Node Hops	No	No	Graphical	No
Nodes	Yes	No	Tabular	No
Packet Stats - Packet Stats	No	No	Graphical	No

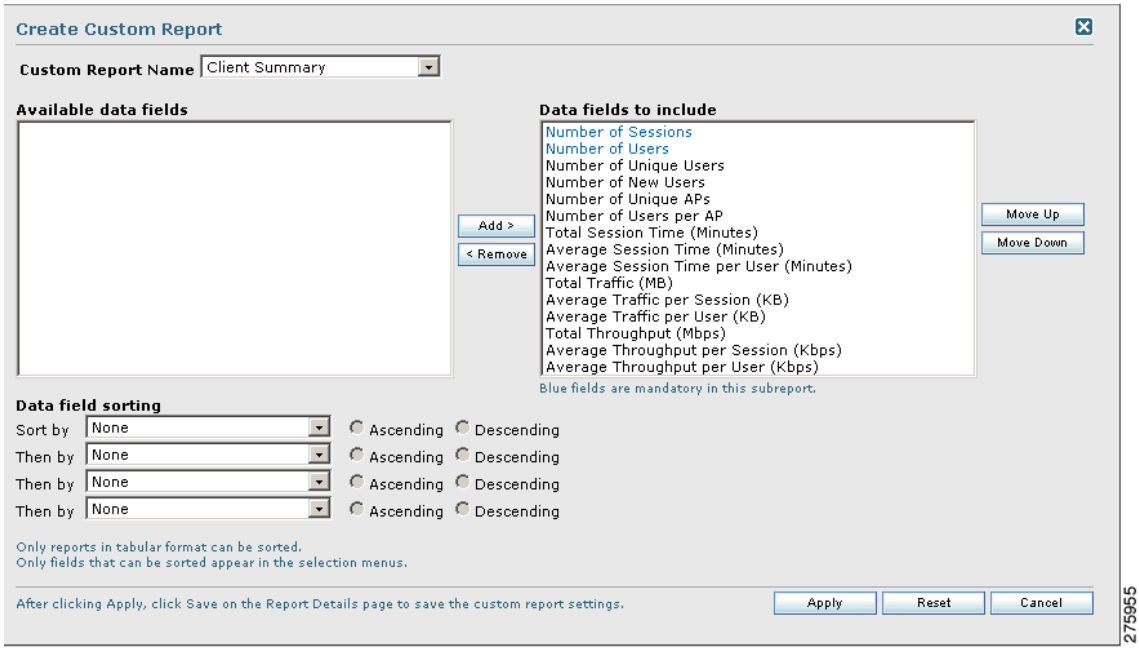
Table 14-2 Report Customization (continued)

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Packet Stats - Packet Error Stats	No	No	Graphical	No
Packet Stats - Packet Queue Stats	No	No	Graphical	No
Stranded APs	No	No	Tabular	No
Worst Node Hops - Worst Node Hop	Yes	Yes	Various	No
Worst Node Hops - Worst SNR Link	Yes	Yes	Various	No
802.11n Summary	No	Yes	Graphical	No
Executive Summary	No	Yes	Various	No
802.11 Counters	Yes	No	Both	Yes
Coverage Holes	Yes	No	Tabular	No
Network Utilization	Yes	Yes	Both	Yes
Traffic Stream Metrics	Yes	Yes	Both	Yes
Tx Power and Channel	No	No	Graphical	No
VoIP Calls Graph	No	No	Graphical	No
VoIP Calls Table	No	No	Tabular	No
Voice Statistics	No	No	Graphical	No
Adaptive wIPS Alarm	Yes	No	Tabular	No
Adaptive wIPS Alarm Summary	Yes	No	Both	No
Adaptive wIPS Top 10 APs	Yes	No	Tabular	No
Adhoc Rogue Count Summary	Yes	No	Both	No
Adhoc Rogues	Yes	No	Tabular	No
New Rogue AP Count Summary	Yes	No	Both	No
New Rogue APs	No	No	Graphical	No
Rogue AP Count Summary	Yes	No	Both	No
Rogue APs	Yes	No	Tabular	No
Security Alarm Trending Summary	No	No	Graphical	No

1. Sub-report Client Summary view is tabular only. The rest of the sub-reports such as Client Summary by Protocol have both report views and are customizable to show either tabular, graphical, or both.
2. Combined inventory report now contains APs/Controllers/MSEs/Autonomous APs/Switches. Reports that are by model or version have both views. These views are customizable with setting such as Count of Controllers by Model. Other reports, such as Controller Inventory, are tabular only.

Step 6 Click **Customize** to open a separate Create Custom Report page (see Figure 14-3).

Figure 14-3 Customize Report View Page



a. From the Custom Report Name drop-down list, choose the report you intend to customize. The Available and Selected column heading selections may change depending on the report selected.

b. From the Report View drop-down list, specify if the report will appear in tabular, graphical, or combined form (both). This option is not available on every report.

c. Use the **Add >** and **< Remove** buttons to move highlighted column headings between the two panes (Available data fields and Data fields to include).

Note Column headings in blue are mandatory in the current sub report. They cannot be removed from the Selected Columns area.

d. Use the **Change Order** buttons (Move Up or Move Down) to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.

e. In the **Data field Sorting** section, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.

- You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to choose each data field for sorting.
- For each sorted data field, choose whether you want it sorted in Ascending or Descending order.

Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

Note The Sortable fields displayed in the Customize page would list out all sortable fields irrespective of the data fields which are in the Data fields to include pane. The Report will be sorted based on the data field selected even if that column is not displayed in the report.

f. Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.

Note The changes made in the Create Custom Report page are not saved until you click **Save** on the Report Details page.

Step 7 When all report parameters have been set, choose one of the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

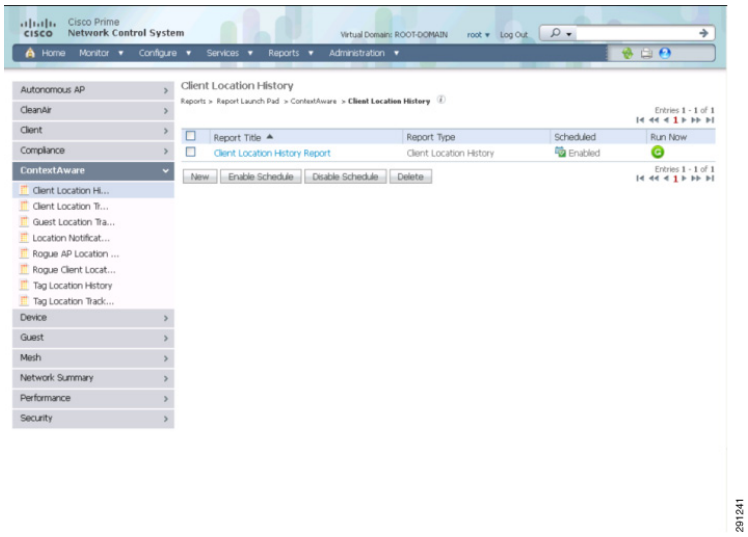
To access current or saved report templates from the Report Launch Pad or Saved Report Template, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

Step 2 Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The page displays a list of current reports for this report type (see Figure 14-4).

Note To view a list of saved report templates, choose **Reports > Saved Report Templates**. See the "Managing Saved Report Templates" section on page 14-16 for more information.

Figure 14-4 Current Reports Page

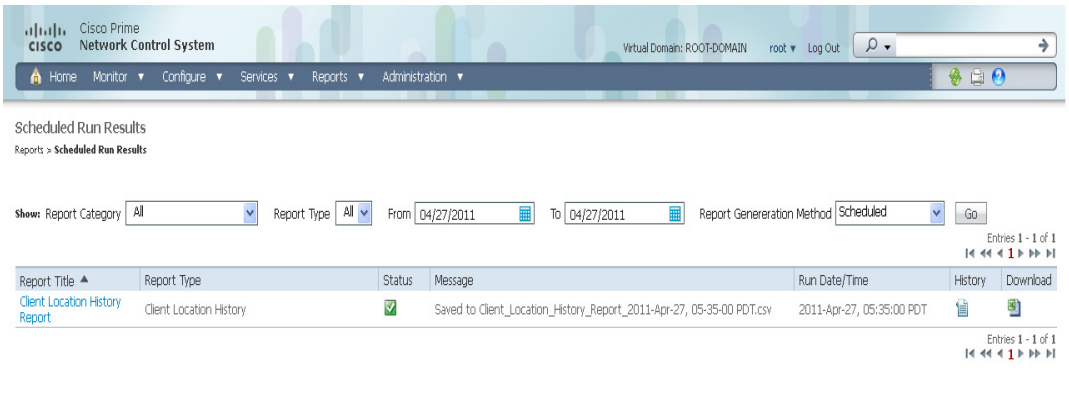


Managing Scheduled Run Results

To view all currently scheduled runs in NCS, choose **Report > Scheduled Run Results** (see Figure 14-5).

Note The list of scheduled runs can be sorted by report category, report type, and time frame.

Figure 14-5 Scheduled Run Results Page



The Scheduled Run Results page displays the following information:

- Report Title—Identifies the user-assigned report name.

Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Status—Indicates whether or not the report ran successfully.
- Message—Indicates whether or not this report was saved and the file name for this report (if saved).
- Run Date/Time—Indicates the date and time that the report is scheduled to run.
- History—Click the History icon to view all scheduled runs and their details for this report.
- Download—Click the Download icon to open or save a .csv/.pdf file of the report results.

For more information about scheduled run results, see the following:

- Sorting Scheduled Run Results, page 14-15
- Viewing or Editing Scheduled Run Details, page 14-16

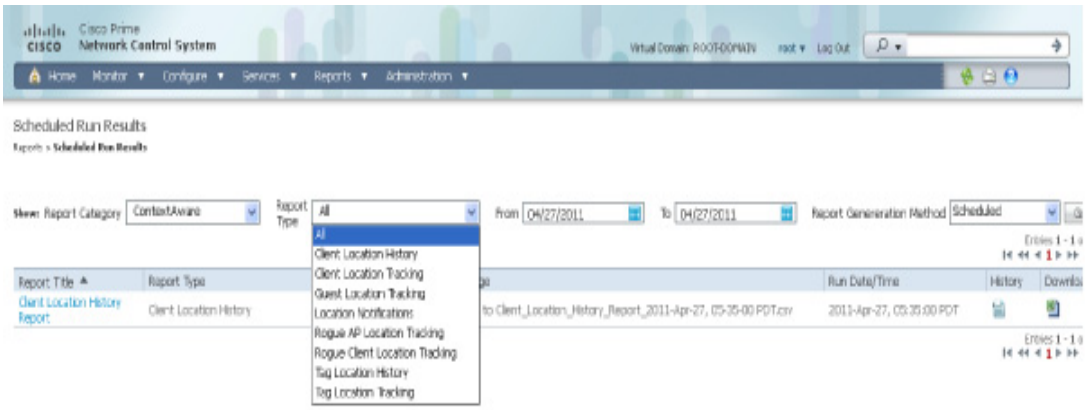
Sorting Scheduled Run Results

You can use the Show drop-down lists to sort the Scheduled Run Results by category, type, and time frame (see Figure 14-6):

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The report Type selections change depending on the selected report category.
- From/To—Type the report start (From) and end (To) dates in the text boxes or click the calendar icons to select the start and end dates.

Click **Go** to sort this list. Only reports that match your criteria appear.

Figure 14-6 Sorting Scheduled Run Results



Viewing or Editing Scheduled Run Details

To view or edit a saved report template, follow these steps:

Step 1 Choose **Report > Scheduled Run Results**.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 From this page, you can view or edit the details for the scheduled run.

Step 4 When all scheduled run parameters have been edited (if necessary), select from the following:

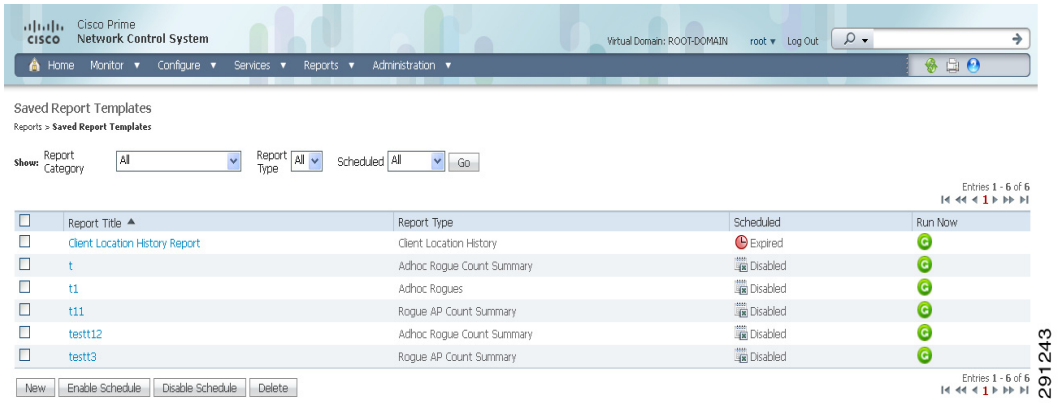
- Save—Click to save this schedule run without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this scheduled run and to immediately run the report.
- Cancel—Click to return to the previous page without running nor saving this report.
- Delete—Click to delete the current saved report template.

Managing Saved Report Templates

In the Saved Report Templates page, you can create and manage saved report templates (see Figure 14-7). To open this page in NCS, choose **Reports > Saved Report Templates**.

Note The list of saved report templates can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired).

Figure 14-7 Saved Report Templates Page



The Saved Report Templates page displays the following information:

- Report Title—Identifies the user-assigned report name.

Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Run—Click the **Run** icon to immediately run the current report.

This section consists of the following topics:

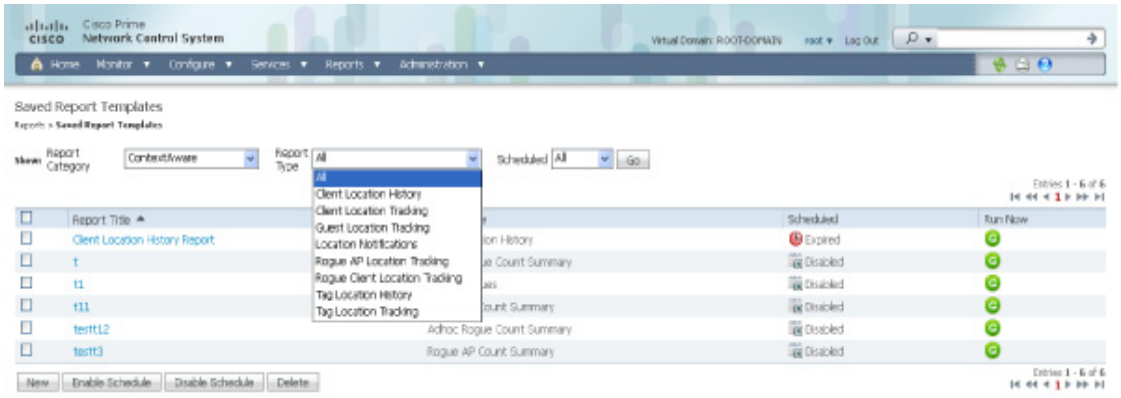
- Filtering Saved Report Templates, page 14-17
- Viewing or Editing Saved Report Template Details, page 14-18
- Running a Saved Report Template, page 14-18

Filtering Saved Report Templates

You can use the Show drop-down lists to filter the Saved Report Templates list by category, type, and scheduled status (see Figure 14-8).

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Choose **All**, **Enabled**, **Disabled**, or **Expired** to filter the Saved Report Templates list by scheduled status.

Figure 14-8 Filtering Saved Report Templates



Click **Go** to filter this list. Only reports that match your criteria appear.

Viewing or Editing Saved Report Template Details

To view or edit a saved report template, follow these steps:

Step 1 Choose **Report > Saved Report Templates**.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 From this page, you can view or edit the details for the saved report template.

Step 4 When all report parameters have been edited, choose one of the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.
- Delete—Click to delete the current saved report template.

Running a Saved Report Template

In the Reports > Saved Report Templates page, click **Run** for the appropriate report. A list of reports specific to NCS follows.

- Autonomous AP Reports
  - Autonomous AP Memory and CPU Utilization
  - Autonomous AP Summary
  - Autonomous AP Tx Power and Channel
  - Autonomous AP Uptime
  - Autonomous AP Utilization
  - Busiest Autonomous APs

- CleanAir Reports
  - Air Quality vs Time
  - Security Risk Interferers
  - Worst Air Quality APs
  - Worst Interferers
- Client Reports
  - Busiest Clients
  - Client Count
  - Client Sessions
  - Client Summary
  - Client Traffic
  - Client Traffic Stream Metrics
  - Posture Status Count
  - Throughput
  - Unique Clients
  - V5 Client Statistics
- Compliance Reports
  - Configuration Audit
  - PCI DSS Detailed
  - PCI DSS Summary
- ContextAware Reports
  - Client Location History
  - Client Location Tracking
  - Guest Location Tracking
  - Location Notifications
  - Rogue AP Location Tracking
  - Rogue Client Location Tracking
  - Tag Location History
  - Tag Location Tracking
- Device Reports
  - AP Image Predownload
  - AP Profile Status
  - AP Summary
  - Busiest APs
  - CPU Utilization
  - Detailed Switch Inventory
  - Identity Capability
  - Inventory

  - Memory Utilization
  - Switch Interface Utilization
  - Uptime
  - Utilization
- Guest Reports
  - Guest Accounts Status
  - Guest Association
  - Guest Count
  - Guest User Sessions
  - NCS Guest Operations
- Identity Services Engine Reports
- Mesh Reports
  - Alternate Parent
  - Link Stats
  - Nodes
  - Packet Stats
  - Packet Error Statistics
  - Packet Queue Statistics
  - Stranded APs
  - Worst Node Hops
- Network Summary
  - 802.11n Summary
  - Executive Summary
- Performance Reports
  - 802.11 Counters
  - Coverage Hole
  - Network Utilization
  - Traffic Stream Metrics
  - Tx Power and Channel
  - VoIP Calls Graph
  - VoIP Calls Table
  - Voice Statistics
- Security Reports
  - Adaptive wIPS Alarm
  - Adaptive wIPS Alarm Summary
  - Adaptive wIPS Top 10 AP
  - Adhoc Rogue Count Summary
  - Adhoc Rogues

- New Rogue AP Count Summary
- New Rogue APs
- Rogue AP Count Summary
- Rogue Access Point Events
- Rogue APs
- Security Alarm Trending Summary

Autonomous AP Reports

This section lists and describes the various Autonomous AP reports that you can generate in NCS. Click **New** next to the Autonomous AP report category to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

The following Autonomous AP reports are available in NCS:

- Autonomous AP Memory and CPU Utilization
- Autonomous AP Summary
- Autonomous AP Tx Power and Channel
- Autonomous AP Uptime
- Autonomous AP Utilization
- Busiest Autonomous APs

Autonomous AP Memory and CPU Utilization

This report displays the memory and CPU utilization trends of Autonomous APs based on the filtering criteria specified during report generation. It could help in identifying unexpected behavior or issues with network performance.

This section contains the following topics:

Configuring an Autonomous AP Memory and CPU Utilization Report

This section describes how to configure an Autonomous AP Memory and CPU Utilization report.

Settings

The following settings can be configured for a Autonomous AP Memory and CPU Utilization report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By

  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

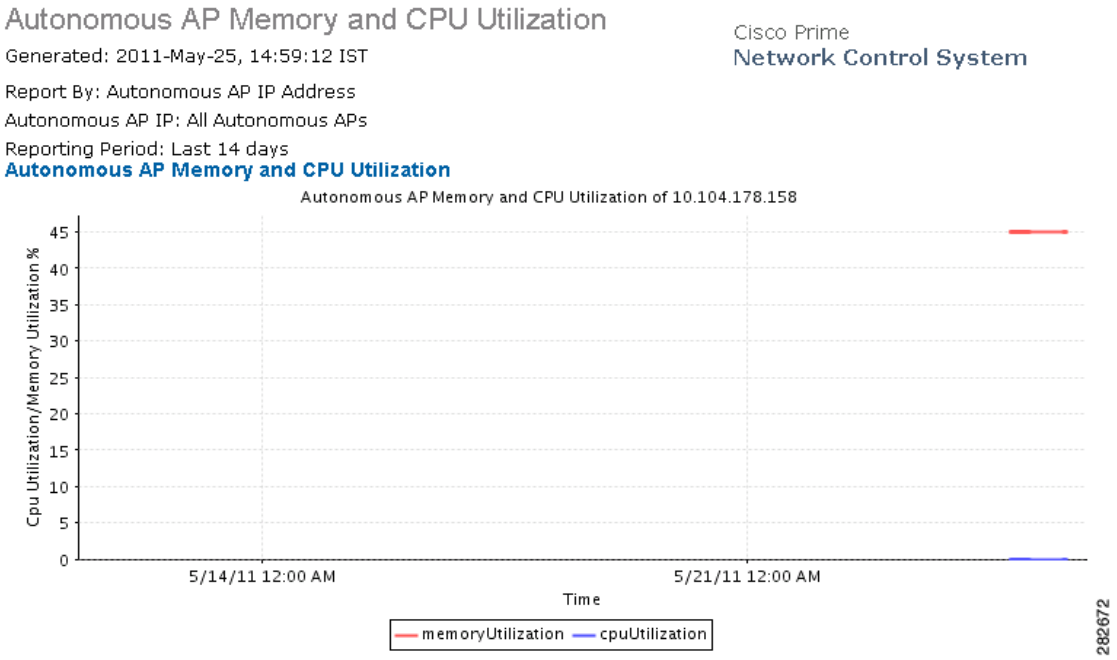
Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Memory and CPU Utilization Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Figure 14-9 shows the potential results for an Autonomous AP Memory and CPU Utilization report, depending on how the report is customized.

Figure 14-9 Autonomous AP Memory and CPU Utilization Report



Autonomous AP Summary

This report displays the Autonomous AP summary.

This section contains the following topics:

- Configuring the Autonomous AP Summary Report, page 14-23
- Autonomous AP Summary Report Results, page 14-24

Configuring the Autonomous AP Summary Report

This section describes how to configure an Autonomous AP Summary report.

Settings

The following settings can be configured for a Autonomous AP Summary report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** or click **Edit** to choose specific locations.

– Outdoor Area—Choose **All Campuses > All Outdoor Areas** or click **Edit** to choose specific locations.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Summary Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for an Autonomous AP Summary report, depending on how the report is customized:

- AP Name
- Ethernet MAC Address
- AP IP Address
- Model
- Map Location

Autonomous AP Tx Power and Channel

This report displays the channel plan assignment and transmits power level trends of devices based on the filtering criteria used when the report was generated. It could help identify unexpected behavior or issues with network performance.

This section contains the following topics:

Configuring an Autonomous AP Tx Power and Channel Report

This section describes how to configure an Autonomous AP Tx Power and Channel report.

Settings

The following settings can be configured for a Autonomous AP Tx Power and Channel report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP By Floor Area—Choose **All Campuses > All Buildings > All Floors** or click **Edit** to choose specific locations.
  - Autonomous AP By Outdoor Area—Choose **All Campuses > All Outdoor Areas** or click **Edit** to choose specific locations.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

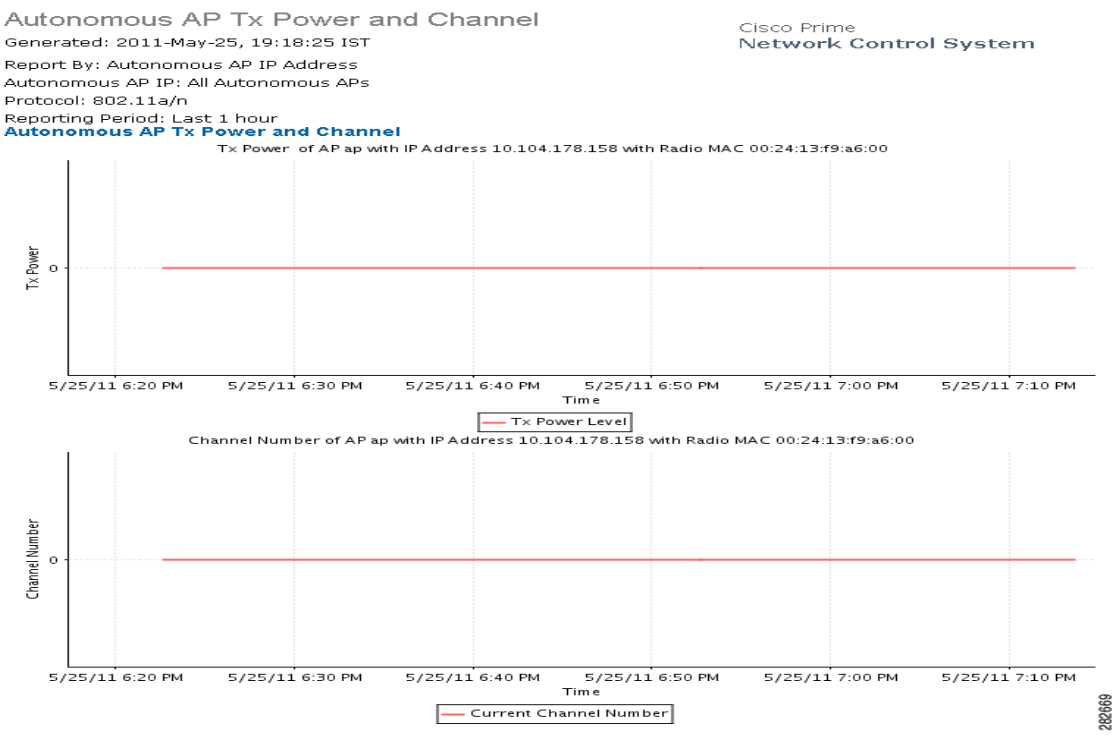
Autonomous AP Tx Power and Channel Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following information is displayed for a Tx Power and Channel report (see Figure 14-10):

- Transmit power level for each access point during the specified period of time.
- Channel number for each access point during the specified period of time.

Figure 14-10 Autonomous AP Tx Power and Channel Report



Autonomous AP Uptime

This report displays the Autonomous AP uptime.

This section contains the following topics:

- Configuring Autonomous AP Uptime Report, page 14-27
- Autonomous AP Uptime Report Results, page 14-28

Configuring Autonomous AP Uptime Report

This section describes how to configure an Autonomous AP Uptime report.

Settings

The following settings can be configured for a Autonomous AP Uptime report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.

  - Autonomous AP By Floor Area—Choose **All Campuses > All Buildings > All Floors** or click **Edit** to choose specific locations.
  - Autonomous AP By Outdoor Area—Choose **All Campuses > All Outdoor Areas** or click **Edit** to choose specific locations.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Uptime Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for an Autonomous AP Uptime report, depending on how the report is customized:

- AP Name
- IP Address
- Map Location

- AP Up Time

Autonomous AP Utilization

This report displays the utilization trends of Autonomous AP radios based on the filtering criteria used when the report was generated. It could help identify current network performance and capacity planning for future scalability needs.

This section contains the following topics:

Configuring an Autonomous AP Utilization Report

This section describes how to configure an Autonomous AP Utilization report.

Settings

The following settings can be configured for a Autonomous AP Utilization report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose **System Campus > All Access Points** or click **Edit** to choose specific access points.
  - Autonomous AP Floor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
  - Autonomous AP Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

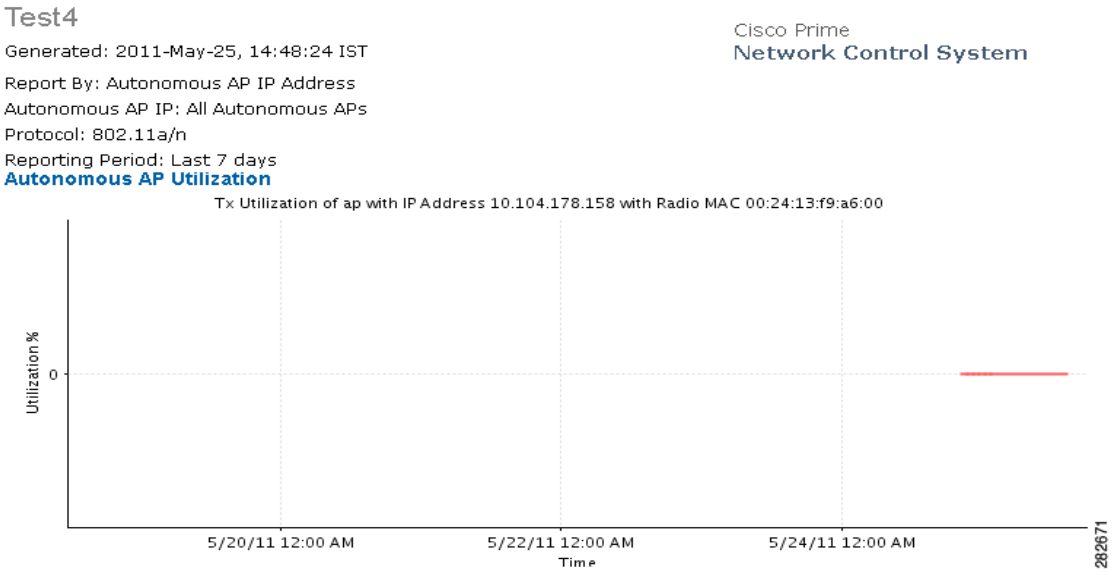
Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Utilization Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Figure 14-11 shows the potential results for an Autonomous AP Utilization report, depending on how the report is customized.

Figure 14-11 Autonomous AP Utilization Report



Busiest Autonomous APs

This report displays the Autonomous APs with the highest total usage (the sum of transmitting, receiving, and channel usage) on your wireless network.

Configuring a Busiest Autonomous APs Report

This section describes how to configure an Busiest Autonomous APs report.

Settings

The following settings can be configured for a Busiest Autonomous APs report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose **System Campus > All Access Points** or click **Edit** to choose specific access points.
  - Autonomous AP Floor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
  - Autonomous AP Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Busiest Autonomous APs Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for an Busiest Autonomous APs report, depending on how the report is customized:

- IP Address
- AP Name
- Rx Utilization (%)
- Tx Utilization (%)

CleanAir Reports

Click **New** for CleanAir report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

This section contains the following CleanAir reports:

- Air Quality vs Time
- Security Risk Interferers
- Worst Air Quality APs
- Worst Interferers

Air Quality vs Time

This report displays the air quality index distributions over a period of time for access points on your wireless networks.

Click **Air Quality vs Time** from the Report Launch Pad to open the Air Quality vs Time page. In this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Air Quality vs Time page. See the "Configuring an Air Quality vs Time Report" section on page 14-33 and the "Air Quality vs Time Report Results" section on page 14-34 for more information.

Configuring an Air Quality vs Time Report

This section describes how to configure an Air Quality vs Time report.

Settings

The following settings can be configured for an Air Quality vs Time report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Controllers > All Access Points**, or click **Edit** to choose specific access points.
  - AP By Floor Area—Choose **System Campus > All Access Points**, or click **Edit** to choose specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points**, or click **Edit** to choose specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Air Quality vs Time Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for an Air Quality vs Time report, depending on how the report is customized:

- AP Name
- MAC Address
- Radio Type
- Time
- AQ Minimum Index
- AQ Average Index

Security Risk Interferers

This report displays the security risk interferers on your wireless network.

Click **Security Risk Interferers** from the Report Launch Pad to open the Security Risks Interferers page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Security Risk Interferers page. See the "Configuring a Security Risk Interferers Report" section on page 14-35 and the "Security Risks Interferers Report Results" section on page 14-36 for more information.

Configuring a Security Risk Interferers Report

This section describes how to configure a Security Risk Interferers report.

Settings

The following settings can be configured for a Security Risks Interferers report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Campuses>All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP By Floor Area—Choose **All Campuses>All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points**, or click **Edit** to choose specific locations or access devices.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Note The information in this report will be available only if you set a security alarm on the interferer.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.

- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Security Risks Interferers Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Security Risks Interferers report, depending on how the report is customized:

- Interferer Type
- Affected Channels
- Discovered
- Last Updated
- Detected AP Name
- Affected Band

Worst Air Quality APs

This report displays the access points with the lowest air quality index.

Click **Worst Air Quality APs** from the Report Launch Pad to open the Worst Air Quality APs page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Air Quality APs page. See the "Configuring a Worst Air Quality APs Report" section on page 14-36 and the "Worst Air Quality APs Report Results" section on page 14-38 for more information.

Configuring a Worst Air Quality APs Report

This section describes how to configure a Worst Air Quality APs report.

Settings

The following settings can be configured for a Worst Air Quality APs report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By

  - AP By Controller—Choose **All Campuses>All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP By Floor Area—Choose **All Campuses>All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points**, or click Edit to choose specific locations or access devices.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Worst Air Quality APs Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Worst Air Quality APs report, depending on how the report is customized:

- AP Name
- Radio Type
- Worst Air Quality Value
- Channel Number
- Most Recent Reported Time
- Interferer Count

Worst Interferers

This report displays the worst interferers on your wireless network.

Click **Worst Interferers** from the Report Launch Pad to open the Worst Air Quality APs page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Interferers page.

Configuring a Worst Interferers Report

This section describes how to configure a Worst Interferers report.

Settings

The following settings can be configured for a Worst Interferers report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Cluster Center AP
  - Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the report criteria area, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Area** from the report criteria area, or click **Edit** to choose specific locations.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.

  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Worst Interferers Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Worst Interferers report, depending on how the report is customized:

- Device Type
- Severity
- Worst Severity Time
- Duty Cycle (%)

- Affected Channels
- Cluster Center APs
- Map Location
- Discovered

Note Severity value N/A means that the severity value for this device is not available. A value of 1 means that the severity is minimal and a value of 100 means very severe.

Note Interferers with unknown location are not listed if the Report By criteria is Floor Area or Outdoor Area.

Client Reports

The report structure has changed in Release 6.0 or later:

- The Client Association and Detailed Client report are replaced by the Client Session report.
- Any saved Detailed Client reports are migrated to the Client Session report.
- Client Association data from 5.1 or earlier is not migrated.

  Note After migration to 6.0 or later releases, you cannot see previous Client Association information that was presented in the Client Association report.

- The Client Count report that was under 802.11 Scaling in release 5.2 is now consolidated into one Client Count report.

The following types of client reports are available:

- Busiest Clients
- Client Count
- Client Sessions
- Client Summary
- Client Traffic Stream Metrics
- Throughput
- Unique Clients
- V5 Client Statistics
- Posture Status Count

Busiest Clients

This report displays the busiest and least busy clients on the wireless network by throughput, utilization, and other statistics. You can sort this report by location, by band, or by other parameters.

Note Busiest Clients reports do *not* include autonomous clients.

Click Busiest Clients from the Report Launch Pad to open the Busiest Clients Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

Configuring a Busiest Client Report

This section describes how to configure a Busiest Client report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page or click **Edit** to choose a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **All Clients**, **Wired Clients**, or a specific radio type from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the clients last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to available columns.

Available information for the Busiest Client report results contains the following:

- Client MAC Address—The MAC address of the client.
- Client IP Address—The IP address of the client.
- Username
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11n_2.4 GHz
- Throughput (Mbps)—The average throughput (in Mbps) for the client.
- Utilization (%)—The average percentage of use for this client.
- On Controller—The controller on which the client is located.
- Bytes Sent—The number of bytes sent.
- Bytes Received—The number of bytes received.
- Packets Sent—The number of packets sent.
- Packets Received—The number of packets received.

Busiest Client Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following potential results occur, depending on how the report is customized (see Figure 14-12):

- Client MAC address, IP address, and username
- Protocol—802.11a/n or 802.11b/g/n
- Throughput—Either Mbps or kbps

  Note If throughput is less than 0.1 kbps, you see <0.1 kbps.

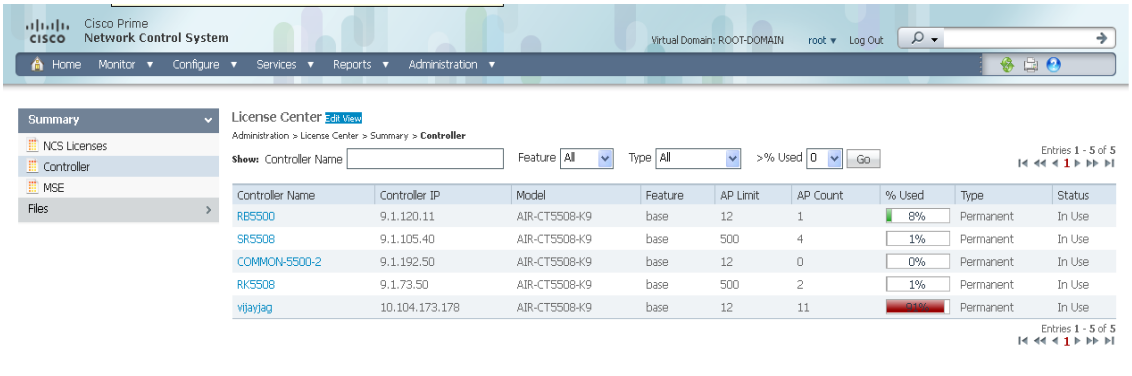
- Utilization (%)
- On Controller—The controller on which the client is located.
- Bytes sent and received

Note If the value is greater than 1,000,000,000, a G is appended at the end of the value (such as 3.45 G). If the value is greater than 1,000,000 but less than 1,000,000,000, an M is appended at the end of the value (such as 456.8 M).

- Packets sent and received

Note If the value is greater than 1,000,000,000, a G is appended at the end of the value (such as 3.45 G). If the value is greater than 1,000,000 but less than 1,000,000,000, an M is appended at the end of the value (such as 456.8 M).

Figure 14-12 Busiest Client Report Results



Client Count

This trending report displays the total number of active clients on your wireless network.

The Client Count report displays data on the numbers of clients that connected to the network through a specific device, in a specific geographical area, or through a specific or multiple SSIDs.

Note Client Count reports include clients connected to autonomous Cisco IOS access points.

Configuring a Client Count Report

This section describes how to configure a Client Count report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.

- Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
- Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
- AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
- AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
- SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
- AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

Note In the Report Criteria page, click **Select** to confirm your sort criteria or **Close** to return to the previous page.

- Protocol—Choose **All Clients** or a specific radio type from the drop-down list.

Note Wired clients and clients associated to Cisco IOS access points are not included as part of this report.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Client Count report results contain the following:

- Controller IP—The IP address of the controller.

- Time—The time the client count occurred.
- Associated Client Count—The number of associated clients for the specified period of time.
- Authenticated Client Count—The number of authenticated clients for the specified period of time.

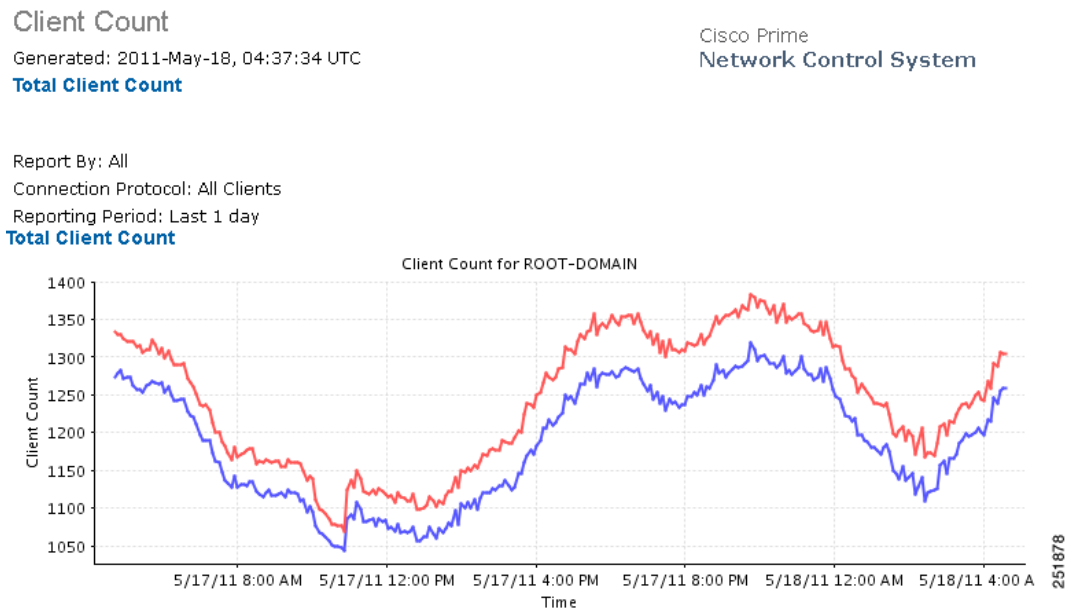
Client Count Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Count report, depending on how the report is customized (see Figure 14-13):

- Client IP address
- AP Name
- Key
- SSID
- Date and time the count was taken
- Associated client count
- Authenticated client count

Figure 14-13 Client Count Report Results



Client Sessions

This report provides client sessions for the given period of time. It displays the history of client sessions, statistics, and the duration at which clients are connected to an access point at any given period of time.

Click **Client Sessions** from the Report Launch Pad to open the Client Sessions Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

Configuring a Client Sessions Report

This section describes how to configure a Client Sessions report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.

  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

  - VLAN
  - Client MAC Address
  - Client Username
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Client Sessions report results contain the following:

- Client Username
- Client IP Address—The IP address of the client.
- Client MAC Address—The MAC address of the client.
- Association Time —The date and time the client associated.

- Vendor—The vendor name for this client.
- AP Name—The access point to which this client is associated.
- Controller Name—The name of the controller to which this client is associated.
- Map Location—The building, floor area, or outdoor area (as applicable) where the client is located.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11b_2.4 GHz.
- Session Duration—The length of time of the client session in hours, minutes, and seconds.
- Policy Type—The type of security policy for this client session.
- Average Session Throughput (kbps)—The average throughput in kbps for this client session.
- Host Name—The DNS host name of the device the client is on. NCS does a DNS lookup to resolve the host name from the IP address of the client. The IP address to host name mapping must be defined in a DNS server. By default, the host name lookup is disabled. Use Administration > Settings > Clients to enable host name lookup.
- CCX—The Cisco Client Extension version number.
- AP MAC Address
- IP address
- AP Radio—The radio type of the access point.
- Controller IP Address—The IP address of the controller to which this client is associated.
- Controller Port—The port number for the controller to which this client is associated.
- Anchor Controller—The IP address of the anchor or foreign controller for the mobility client.
- Association ID
- Disassociation Time—The date and time this client disassociated.
- Authentication—The authentication method for this client.
- Encryption Cipher
- EAP Type
- Authentication Algorithm
- Web Security
- Tx and Rx (bytes)—The approximate number of bytes transmitted or received during the session.

Client Sessions Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

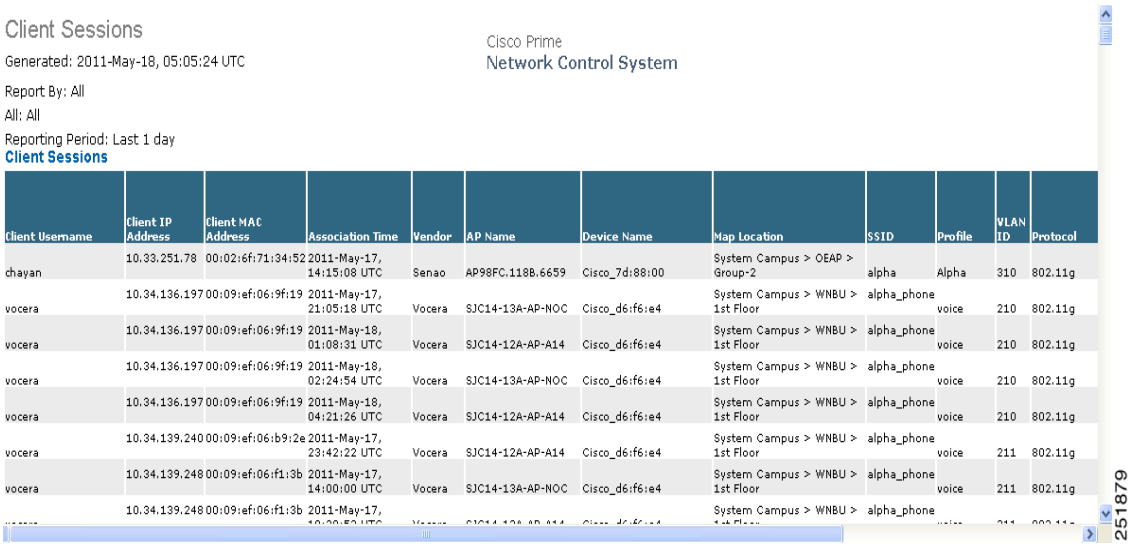
The following are potential results for a Client Sessions report, depending on how the report is customized (see Figure 14-14):

- Client username, IP address, and MAC address (mandatory columns)

- Association time (mandatory column)
- Vendor
- Access point name—The access point name to which this client is assigned.
- Controller names
- Map Location—The building, floor area, or outdoor area (as applicable) where the client is located.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5GHz, or 802.11b_2.4GHz.
- Session Duration
- Policy Type—The type of security policy for this client session.
- Average Session Throughput (kbps)
- Host Name—The DNS host name of the machine on which this client is located.

  NCS performs an DNS lookup to resolve the host name from the client IP address. The IP address to host name mapping must be defined in a DNS server. By default, the host name lookup is disabled. You can enable it from the Administration > Settings > Clients page.
- CCX—The Cisco Client Extension version number.
- AP MAC address
- IP address
- AP Radio—The radio type of the access point.
- Controller IP address
- Controller Port—The port number for the controller to which this client is associated.
- Anchor Controller—The IP address of the anchor or foreign controller for the mobility client, if applicable.
- Association ID—Association ID used in this client session.
- Disassociation Time—The date and time this client disassociated.
- Authentication—The authentication method for this client.
- Encryption Cypher—Encryption cypher used in this client session.
- EAP Type—EAP type used in this client session.
- Authentication Algorithm—Authentication algorithm used in this client session.
- Web Security—Web security used in this client session.
- Tx and Rx (bytes)—The approximate number of bytes transmitted or received during the client session.
- Packets sent and received
- SNR—Signal-to-noise ratio for this client session.
- RSSI—The received signal strength indicator in dBm.
- Status—Associated or disassociated.
- Reason—Reason for disassociation.
- E2E—Version number or *Not Supported*.

Figure 14-14 Client Sessions Report Results



Client Sessions

Generated: 2011-May-18, 05:05:24 UTC

Report By: All

All: All

Reporting Period: Last 1 day

Cisco Prime
Network Control System

Client Sessions

Client Username	Client IP Address	Client MAC Address	Association Time	Vendor	AP Name	Device Name	Map Location	SSID	Profile	VLAN ID	Protocol
chayan	10.33.251.78	00:02:6f:71:34:52	2011-May-17, 14:15:08 UTC	Senao	AP98FC.118B.6659	Cisco_7d:88:00	System Campus > OEAP > Group-2	alpha	Alpha	310	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-17, 21:05:18 UTC	Vocera	SJC14-13A-AP-NOC	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-18, 01:08:31 UTC	Vocera	SJC14-12A-AP-A14	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-18, 02:24:54 UTC	Vocera	SJC14-13A-AP-NOC	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-18, 04:21:26 UTC	Vocera	SJC14-12A-AP-A14	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.139.240	00:09:ef:06:b9:2e	2011-May-17, 23:42:22 UTC	Vocera	SJC14-12A-AP-A14	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	211	802.11g
vocera	10.34.139.248	00:09:ef:06:f1:3b	2011-May-17, 14:00:00 UTC	Vocera	SJC14-13A-AP-NOC	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	211	802.11g
	10.34.139.248	00:09:ef:06:f1:3b	2011-May-17,				System Campus > WNBU >	alpha_phone			

251879

Client Summary

The Client Summary is a detailed report that displays various client statistics.

Click Client Summary from the Report Launch Pad to open the Client Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

Note You cannot upgrade the settings for the Client Summary report from WCS 7.x to NCS 1.0.

Configuring a Client Summary Report

This section describes how to configure a Client Summary report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Note The data for client summary report is computed at backend. The report uses the computed data only. The data is computed every hour for one day and every night for a year. Thus you would only be able to create hourly-based client summary reports for the last 24 hours.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note A Client Summary report contains summary results sorted by protocol, SSID, VLAN, and vendor. To customize report results for a particular section, choose the applicable section from the Customizable Report drop-down list.

The Client Summary report contains four sub reports. Each of them can be independently customized. The following is default information available from a Client Summary report depending on the customizable report selected:

- Number of Sessions
- Number of Total Users
- Number of Unique Users
- Number of New Users
- Number of Unique APs
- Number of Users per AP
- Total Traffic (MB)
- Average Traffic per Session (KB) and per user (in KB)
- Total Throughput (Mbps)
- Average Throughput per Session and per user (Mbps)

  Note When NCS does not receive client traps, it relies on client status polling to discover client associations (The task runs every 5 minutes by default.). However, NCS cannot accurately determine when the client was actually associated. NCS assumes the association started at the polling time which may be later than the actual association time. Therefore the calculation of the average client throughput can give inaccurate results, especially for short client sessions.

- Protocol—802.11a/n or 802.11b/g/n.
- SSID—The user-defined Service Set Identifier name

- VLAN
- Vendor
- User Count
- Time Used (Minutes)
- Traffic (MB)
- Session Count
- % of Users
- % of Time
- % of Traffic
- % of Session
- Total Time of a session

Client Summary Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Summary report, depending on how the report is customized (see Figure 14-15):

Client Summary

- Number of Sessions (mandatory column)
- Number of Total Users (mandatory column)—Number of unique endpoints or MAC addresses.
- Number of Unique Users—Number of unique user names that are authenticated.
- Number of New Users
- Number of Unique Access Points
- Number of Users per Access Point
- Total session time in minutes
- Total traffic (MB)
- Average traffic per session (KB) and per user (in KB)
- Total throughput (MBPS)
- Average throughput per session and per user (MBPS)

Note When NCS does not receive client traps, it relies on client status polling to discover client associations (The task runs every 5 minutes by default). However, NCS cannot accurately determine when the client was actually associated. NCS assumes the association started at the polling time which may be later than the actual association time. Therefore the calculation of the average client throughput can give inaccurate results, especially for short client sessions.

Note NCS only counts authenticated sessions. If a user fails on DHCP or authentication, NCS will not have a session for it. Also, NCS considers every detected AP association as a session. For instance, if a client roams from one access point to another, NCS can have two association sessions.

Client Summary by Protocol, SSID, VLAN, and Vendor

- Protocol (mandatory column)
- SSID (mandatory column)
- VLAN (mandatory column)
- Vendor (mandatory column)
- User Count (mandatory column)
- Time Used (mandatory column)
- Traffic (mandatory column)
- Session Count (mandatory column)
- % of users, time, traffic, and sessions

Figure 14-15 Client Summary Report Results

Client Summary

Generated: 2011-May-17, 04:01:11 UTC

Cisco Prime
Network Control System

Reporting Period: Last 1 day

Client Session Summary

Connection Type	Number of Sessions	Average Number of Clients	Posture passed Daily Count	Posture failed Daily Count	Average Number of Users	Number of New Clients
Lightweight	3117	442	0	0	442	0
Total	3117	442	0	0	442	0

Client Device Summary

Connection Type	Average Number of Devices	Average Clients per Device	Average Sessions per Device	Average Number of APs	Average Clients per AP	Average Sessions per AP
Lightweight	15	29.47	207.8	331	1.34	9.42
Total	15	29.47	207.8	331	1.34	9.42

Client Traffic Summary

Connection Type	Total Session Time (Hours)	Average Session Time (Minutes)	Average Session Time per Client (Minutes)	Total Traffic (MB)	Average Traffic per Session (KB)	Average Traffic per Client (KB)	Total Throughput (Mbps)	Average Throughput per Session (Kbps)	Average Throughput per Client (Kbps)
Lightweight	714.42	13.75	96.98	136430.05	43769.67	308665.28	563609.0	180817.77	1275133.48
Total	714.42	13.75	96.98	136430.05	43769.67	308665.28	563609.0	180817.77	1275133.48

Client Summary by Protocol

Protocol	Number of Sessions	Number of Clients	Session Time (Hours)	Traffic (MB)	% of Sessions	% of Clients	% of Session Time	% of Traffic
802.11g	1280	748	271.85	14791.58	41.07	40.02	38.05	10.84
802.11a	809	523	233.17	58436.33	25.95	27.98	32.64	42.83
802.11n_2.4GHz	489	326	105.78	59001.99	15.69	17.44	14.81	43.25
802.11n_5GHz	313	241	86.72	4200.16	10.04	12.89	12.14	3.08
802.11b	225	30	16.85	0.0	7.22	1.61	2.36	0.0
802.3	1	1	0.0	0.0	0.03	0.05	0.0	0.0

Clients by Protocol

Client Traffic

This report displays the traffic by the wireless clients on your network.

Click **Client Traffic** from the Report Launch Pad to open the Client Traffic Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

Configuring a Client Traffic Report

This section describes how to configure a Client Traffic report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by

  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
- Reporting Period—Specify the time period for which the report needs to be generated. You can choose from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

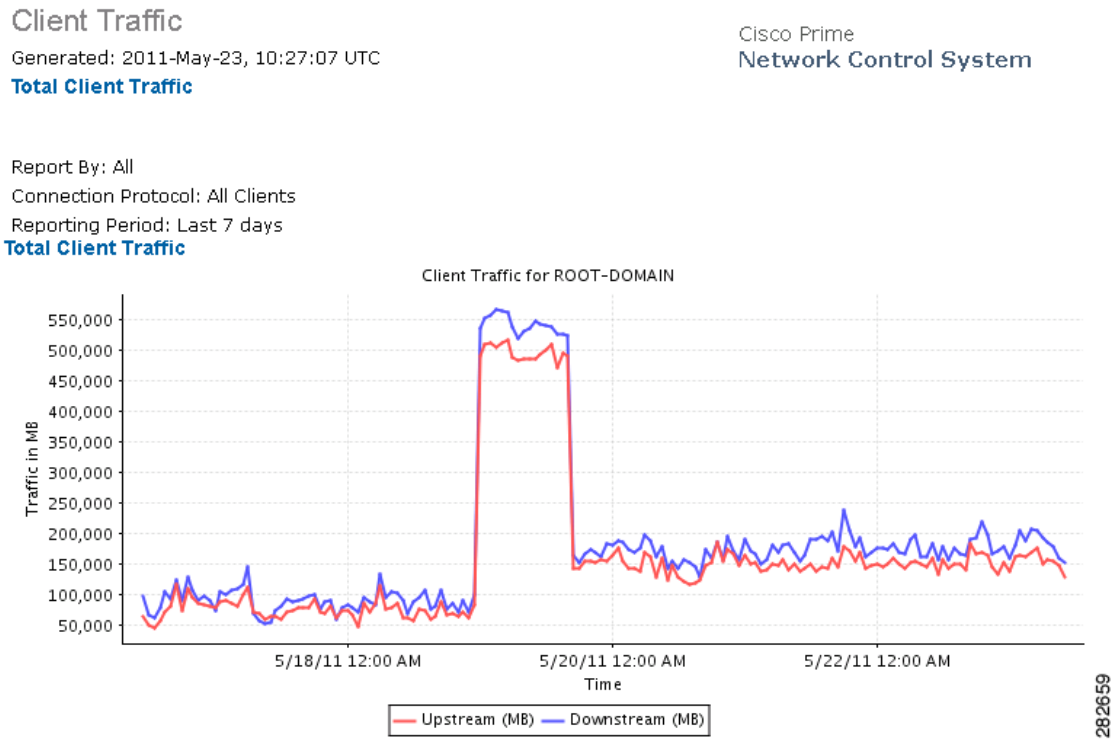
Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Client Traffic Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following figure shows the potential results for a Client Traffic report, depending on how the report is customized (see Figure 14-16).

Figure 14-16 Client Traffic Report Results



Client Traffic Stream Metrics

This report displays Traffic Stream Metrics for clients. You can select from the following:

- All clients of a given set of SSIDs
- All clients
- One specific client

Click **Client Traffic Stream Metrics** from the Report Launch Pad to open the Client Traffic Stream Metrics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Client Traffic Stream Metrics Reports page.

Note The traffic stream metrics and radio performance background tasks must be running prior to generating this report.

Configuring a Client Traffic Stream Metrics Report

This section describes how to configure a Client Traffic Stream Metrics report.

Settings

The following settings can be configured for a Client Traffic Stream Metrics report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
  - Client MAC Address—Choose **All Clients** from the Report Criteria page, or click **Edit** to choose specific clients.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - **Last**—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or client the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Schedule

If you play to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Mandatory columns are displayed in blue font and cannot be moved to Available Columns. Time, Client MAC address, and QoS are mandatory columns for the Client Traffic Stream Metrics report.

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Traffic Stream Metrics report, depending on how the report is customized:

- Time (mandatory column)
- Client MAC (mandatory column)
- QoS (mandatory column)—QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect how the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data is stored at one time.

- AP Name (mandatory column)
- Radio Type (mandatory column)
- Avg Queuing Delay (ms) (Downlink) (mandatory column)—Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes the time for re-tries, if needed.
- Avg Queuing Delay (ms) (Uplink) (mandatory column)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- % Packets > 40ms Queuing Delay (Uplink)—Percentage of queuing delay packets greater than 40 ms.
- % Packets 20ms-40ms Queuing Delay (Uplink)—Percentage of queuing delay packets between 20 ms and 40 ms.
- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the he first packet is received from the new access point after a successful roam.
- Time—Time that the statistics were gathered from the access point(s).
- Client MAC—MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, or PDA and refers to any client attached to the access point collecting measurements.

Client Traffic Stream Metrics Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

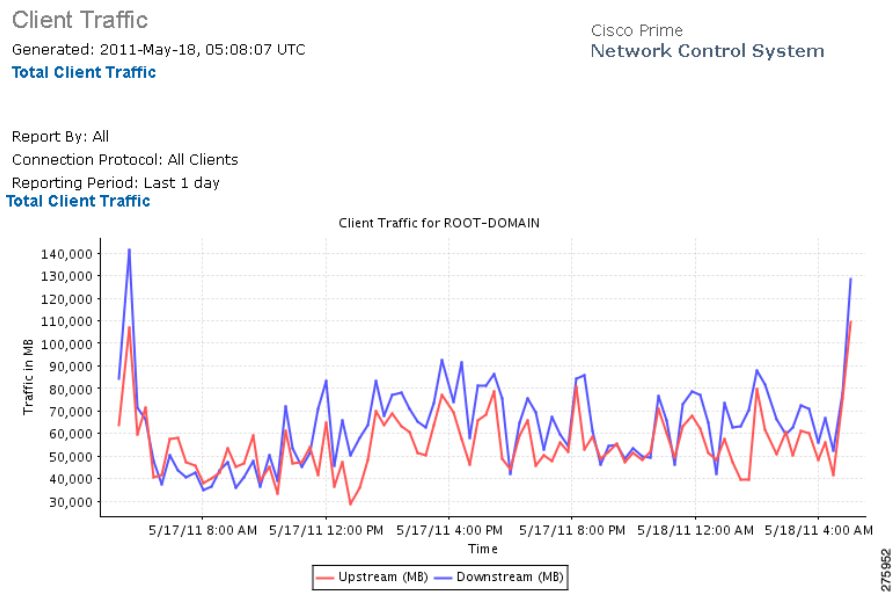
The following are potential results for a Client Traffic Stream Metrics report, depending on how the report is customized (see Figure 14-17):

- Time (mandatory column)
- Client MAC (mandatory column)
- QoS (mandatory column)—QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data per client is stored in the WLC. NCS polls this data and stores it for the last seven days.
- AP Name (mandatory column)
- Radio Type (mandatory column)

- Avg Queuing Delay (ms) (Downlink) (mandatory column)—Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
- Avg Queuing Delay (ms) (Uplink) (mandatory column)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- % Packets > 40ms Queuing Delay (Uplink)—Percentage of queuing delay packets greater than 40 ms.
- % Packets 20ms-40ms Queuing Delay (Uplink)—Percentage of queuing delay packets between 20ms-40 ms.
- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.
- Time—Time that the statistics were gathered from the access point(s).

Client MAC—MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, PDA and refers to any client attached to the access point collecting measurements.

Figure 14-17 Client Traffic Stream Metrics Report Results



Posture Status Count

This trending report displays the failed or succeeded client posture status count on your network.

This section consists of the following topics:

- Configuring a Posture Status Count Report
- Posture Status Count Report Results

Configuring a Posture Status Count Report

This section describes how to configure a Posture Status Count report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

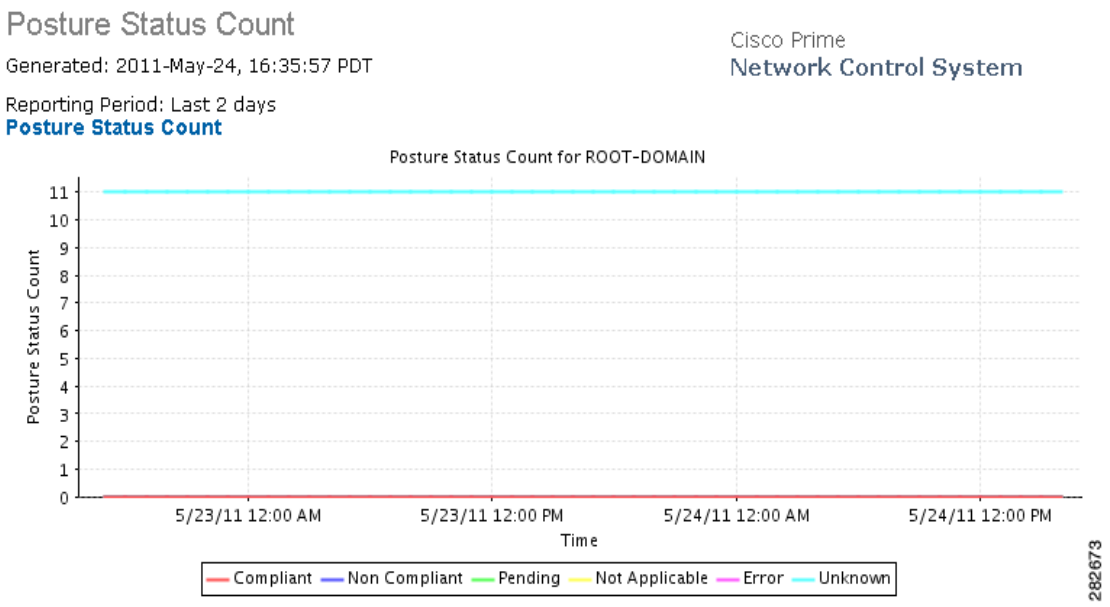
The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Posture Status Count Report Results

The Posture Status Count graph displays the following (see Figure 14-18):

Figure 14-18 Posture Status Count Report



Throughput

This report displays the ongoing bandwidth used by the wireless clients on your network.

Note The Throughput report does not include wired clients or clients connected to Autonomous Cisco IOS access points.

Click **Throughput** from the Report Launch Pad to open the Throughput Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

Configuring a Throughput Report

This section describes how to configure a Throughput report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Controller—Choose **All Controllers > All Access Points** or click **Edit** to choose specific devices.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **All Clients** or a specific radio type from the drop-down list.

  Note Wired clients and clients associated to Cisco IOS access points are not included as part of this report.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

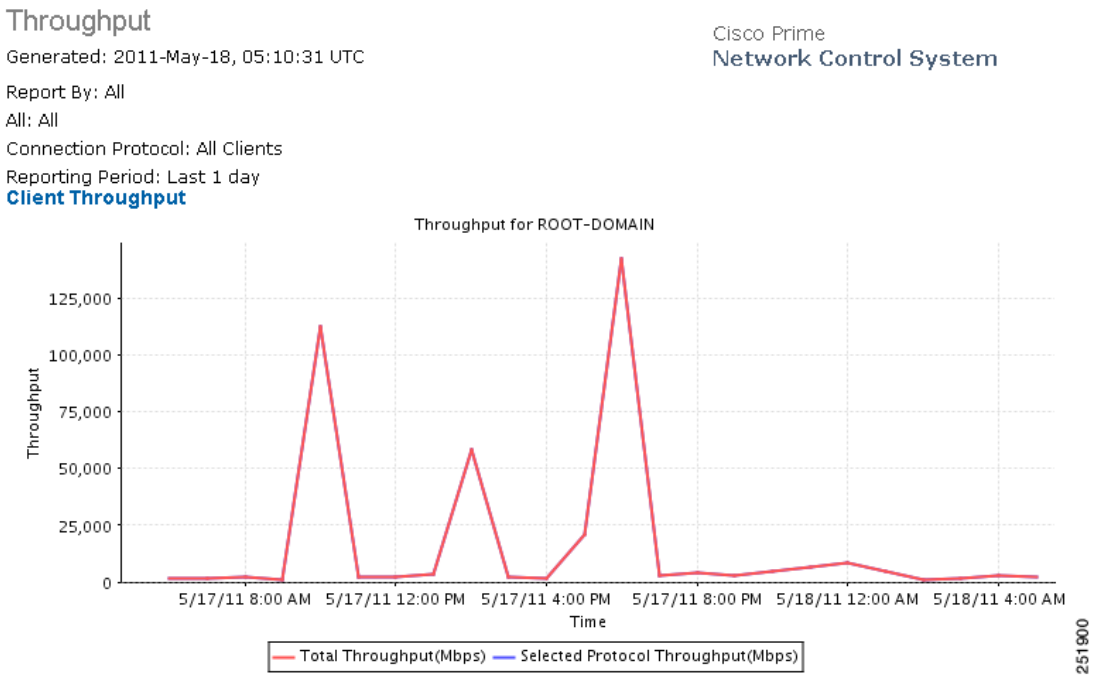
If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Throughput Report Results

The Throughput report graph displays the following (also see Figure 14-19):

- Total throughput (mbps)
- Throughput for the selected protocol
- Date and time for each indicated throughput level

Figure 14-19 Throughput Report Results



Unique Clients

This report displays all unique clients by the time, protocol, and controller filters that you select. A unique clients is determined by the MAC address of the client device. These clients are sorted by controller in this report.

Click **Unique Clients** from the Report Launch Pad to open the Unique Clients Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

A new First Seen column is added in release 6.0. It is the time that NCS first learned of the client MAC address. For existing clients, NCS sets the First Seen column with the timestamp currently in the database, which is the time the record was last updated.

Note The Unique Client report covers any client that started the connection during the specified time period or ended the connection during the specified time period or connected during the specified time period. The specified time period refers to the reporting period that you specify while scheduling the report.

Note Unique Clients reports do ***not*** include autonomous clients.

Configuring a Unique Clients Report

This section describes how to configure a Unique Clients report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **All Clients**, **Wired Clients**, or a specific radio type from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Mandatory columns are displayed in blue font and cannot be moved to Available data fields Column. Last Seen, User, and MAC address are mandatory columns for the Unique Client report.

The following information is available on the unique client report:

- Host Name
- AP MAC Address
- IP Address—The IP address of the controller to which this client is associated.
- Controller IP Address
- Port
- Last Session Length
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- CCX—The Cisco Client Extension version number.
- E2E
- Vendor—The vendor name for this client.
- IP Address
- AP Name—The access point to which this client is associated.
- Controller—The name of the controller to which this client is associated.
- 802.11 State—Client association status.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- Authenticated
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11b_2.4 GHz.
- Map Location

Unique Client Report Results

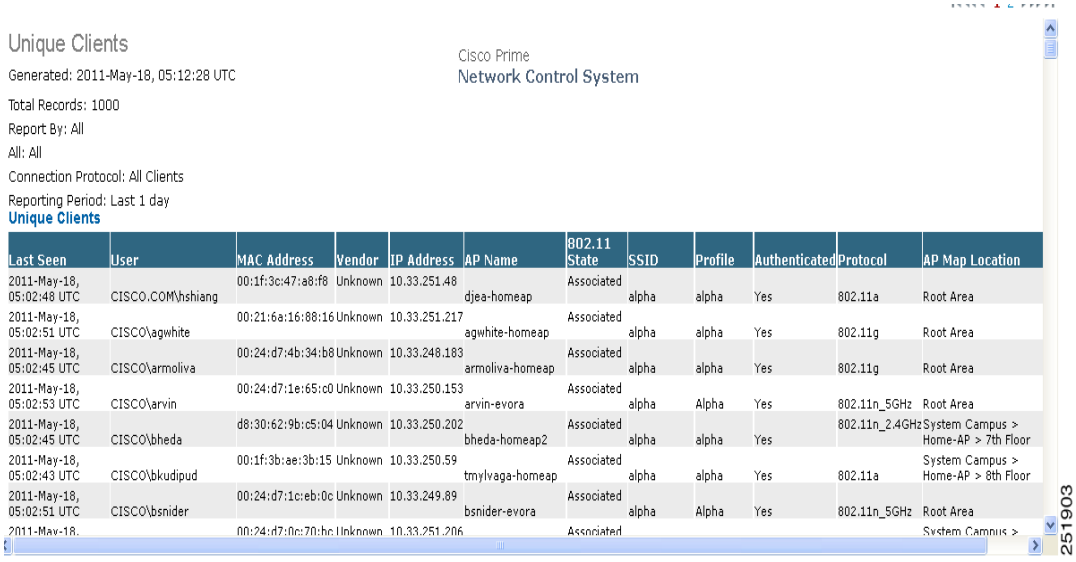
The following information is displayed for a Unique Client report (see Figure 14-20):

- First/Last Seen—Date and time the unique client was first and last viewed
- User—Client username
- Vendor—The vendor name or Unknown
- Client IP Address and MAC Address
- AP Name
- Controller—The controller to which the client was associated
- Port
- 802.11 State—Associated, Disassociated, or Idle
- SSID

Note N/A may display in the SSID field if the client is probing.

- Authenticated—Indicates whether or not the client is authenticated (Yes or No)
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5GHz, or 802.11b_2.4GHz.
- VLAN ID
- CCX—Indicates whether or not CCX (Cisco Client Extensions) is supported.
- E2E—Indicates whether or not E2E (End to End) is supported.
- Map Location

Figure 14-20 Unique Client Report Results



V5 Client Statistics

This report displays the 802.11 and security statistics for Cisco Compatible Extensions v5 clients.

Click **V5 Client Statistics** from the Report Launch Pad to open the V5 Client Statistics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

Configuring a V5 Client Statistics Report

This section describes how to configure a V5 Client Statistics report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

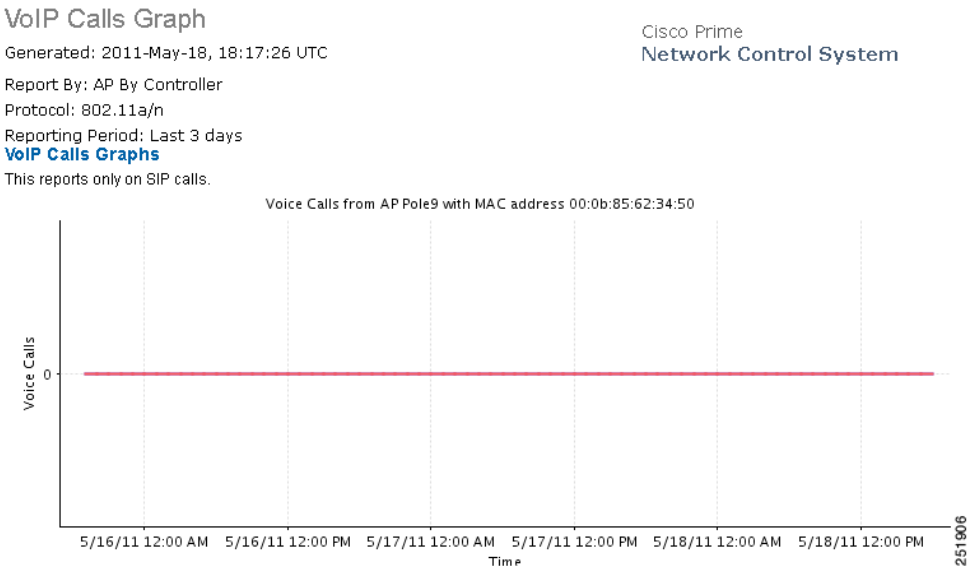
V5 Client Statistics Report Results

The following information is displayed for the v5 Client Statistics report (see Figure 14-21):

- Client MAC Address
- Transmitted Fragment Count—This counter is incremented for each successfully received MPDU Data or Management type.
- Multicast Transmitted Frame Count—This counter increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this implies having received an acknowledgment to all associated MPDUs.
- Failed Count—This counter increments when an MSDU is unsuccessfully transmitted.
- Retry Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Multicast Retry Count—This counter increments when an MSDU is successfully transmitted after more than one retransmission.
- Frame Duplicate Count—This counter increments when a frame is received that the Sequence Control field indicates is a duplicate.

- RTS Success Count—This counter increments when a CTS (clear-to-send) is received in response to an RTS (ready-to-send).
- RTS Fail Count—This counter increments when a clear-to-send is not received in response to a ready-to-send.
- ACK Fail Count—This counter increments when an ACK is not received when expected.
- Received Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- Multicast Received Frame Count—This counter increments when a MSDU is received with the multicast bit set in the destination MAC address.
- FCS Error Count—This counter increments when an Frame Check Sequence error is detected in a received MPDU.
- Transmitted Frame Count—This counter increments for each successfully transmitted MSDU.

Figure 14-21 V5 Client Statistics Report Results



Compliance Reports

The Configuration Audit report displays the differences between NCS and its controllers. The PCI DSS Compliance report summarizes your Wireless LAN Security components with reference to the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. PCI DSS compliance is required for all merchants and service providers that store, process, or transmit cardholder data. You can find PCI DSS standards at the PCI Security Standards Council website.

The following Compliance Reports are available:

- Configuration Audit
- PCI DSS Detailed

- PCI DSS Summary

Configuration Audit

This report displays the configuration differences between NCS and its controllers. You must configure audit mode on the Administration > Settings page. In audit mode, you can perform an audit based on templates or the stored configuration. The report shows the last time an audit was performed using the Configuration Sync background task.

Click **Configuration Audit** from the Report Launch Pad to open the Configuration Audit Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Configuration Reports page. See the "Configuring a Configuration Audit Report" section on page 14-69 and the "Configuration Audit Report Results" section on page 14-70 for more information.

Configuring a Configuration Audit Report

This section describes how to configure a Configuration Audit report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Controller—Choose **All Controllers** or a specific controller from the available list.
- Audit Time—Choose **Latest** or a specific date and time from the available list.

Note The available audit times are based on when the Configuration Sync background task was run.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note A Configuration Audit report contains the following sections: Audit Summary, Applied Templates and Config Group Template Discrepancies, Enforced Values, Failed Enforcements, and NCS Config Discrepancies. Choose the applicable report from the Customizable Report drop-down list.
To customize report results for a particular section, choose the applicable section from the Customizable Report drop-down list.

A Configuration Audit report contains the following default information, depending on which customized report is selected:

- Controller Name
- Audit Status
- Audit Time
- Name
- Audit Object Display Name
- Device Sync State
- Time
- Client MAC Address
- IP Address
- Message
- Description
- Attribute
- Attribute Value in NCS
- Attribute Value in Device
- Enforced Value
- Instance Name
- Description
- Error Message
- Attribute Value in DB

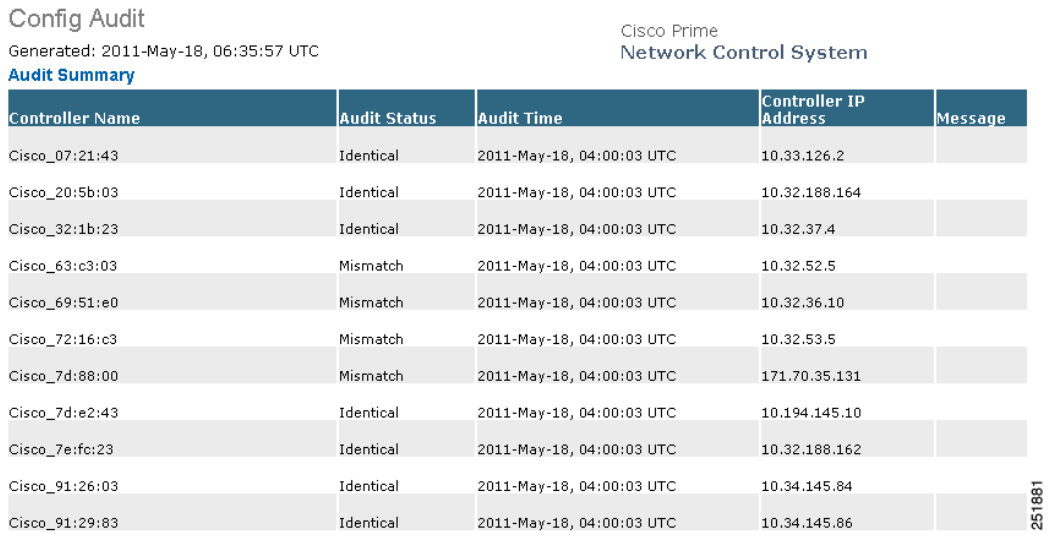
Configuration Audit Report Results

The following are potential results for a Configuration Audit report, depending on how the report is customized (see Figure 14-22):

- Audit Summary results
  - Controller Name (mandatory column)

  - Audit Status (mandatory column)—Not Available (no audit occurred on this switch), Identical (no configuration differences were discovered), Mismatch (configuration differences were discovered).
  - Audit Time (mandatory column)—The time when the network audit background task was run via Configuration Sync task.
  - IP Address—The IP address of the audited controller.
  - Message—It reports “Device unreachable” if the device is unreachable. Also, if any exceptions is found during the audit, it reports “Internal Exception, check the log files”.
- Applied Templates and Config Group Template Discrepancies results
  - Name (mandatory column)
  - Template Name (mandatory column)
  - Audit Status (mandatory column)—(Mismatch, Identical, Not Available)
  - Template Applied Via—Template description.
  - Attribute
  - NCS Value
  - Controller Device
- Enforced Values results
  - Name (mandatory column)
  - Template Name (mandatory column)
  - Audit Status (mandatory column)
  - Template Applied Via
  - Attribute
  - Enforced Value
  - Controller Value
- Failed Enforcements results
  - Name (mandatory column)
  - Object Name
  - Description
  - Error Message
- NCS Config Discrepancies results
  - Controller Name (mandatory column)
  - Object Name (mandatory column)
  - Audit Status (mandatory column)
  - Attribute (mandatory column)
  - NCS Value
  - Controller Value

Figure 14-22 Configuration Audit Report Results



Config Audit

Generated: 2011-May-18, 06:35:57 UTC

Cisco Prime
Network Control System

Audit Summary

Controller Name	Audit Status	Audit Time	Controller IP Address	Message
Cisco_07:21:43	Identical	2011-May-18, 04:00:03 UTC	10.33.126.2	
Cisco_20:5b:03	Identical	2011-May-18, 04:00:03 UTC	10.32.188.164	
Cisco_32:1b:23	Identical	2011-May-18, 04:00:03 UTC	10.32.37.4	
Cisco_63:c3:03	Mismatch	2011-May-18, 04:00:03 UTC	10.32.52.5	
Cisco_69:51:e0	Mismatch	2011-May-18, 04:00:03 UTC	10.32.36.10	
Cisco_72:16:c3	Mismatch	2011-May-18, 04:00:03 UTC	10.32.53.5	
Cisco_7d:88:00	Mismatch	2011-May-18, 04:00:03 UTC	171.70.35.131	
Cisco_7d:e2:43	Identical	2011-May-18, 04:00:03 UTC	10.194.145.10	
Cisco_7e:fc:23	Identical	2011-May-18, 04:00:03 UTC	10.32.188.162	
Cisco_91:26:03	Identical	2011-May-18, 04:00:03 UTC	10.34.145.84	
Cisco_91:29:83	Identical	2011-May-18, 04:00:03 UTC	10.34.145.86	

251881

PCI DSS Detailed

This report displays the PCI Data Security Standard (DSS) version 2.0 requirements in detail that are relevant to your wireless network security.

Click **PCI DSS Detailed** from the Report Launch Pad to open the PCI DSS Detailed Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the PCI DSS Detailed Reports page. See the "Configuring a PCI DSS Detailed Report" section on page 14-72 and the "PCI DSS Detailed Report Results" section on page 14-73 for more information.

Configuring a PCI DSS Detailed Report

This section describes how to configure a PCI DSS Detailed report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By

- Controller—Choose **All Controllers** from the Report Criteria box or click **Edit** to choose specific devices.
- MSE—Choose **All MSEs** from the Report Criteria box or click **Edit** to choose a specific MSE.
- Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria box or click **Edit** to choose specific locations.

Note In the Filter Criteria box, choose the appropriate filter criteria.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

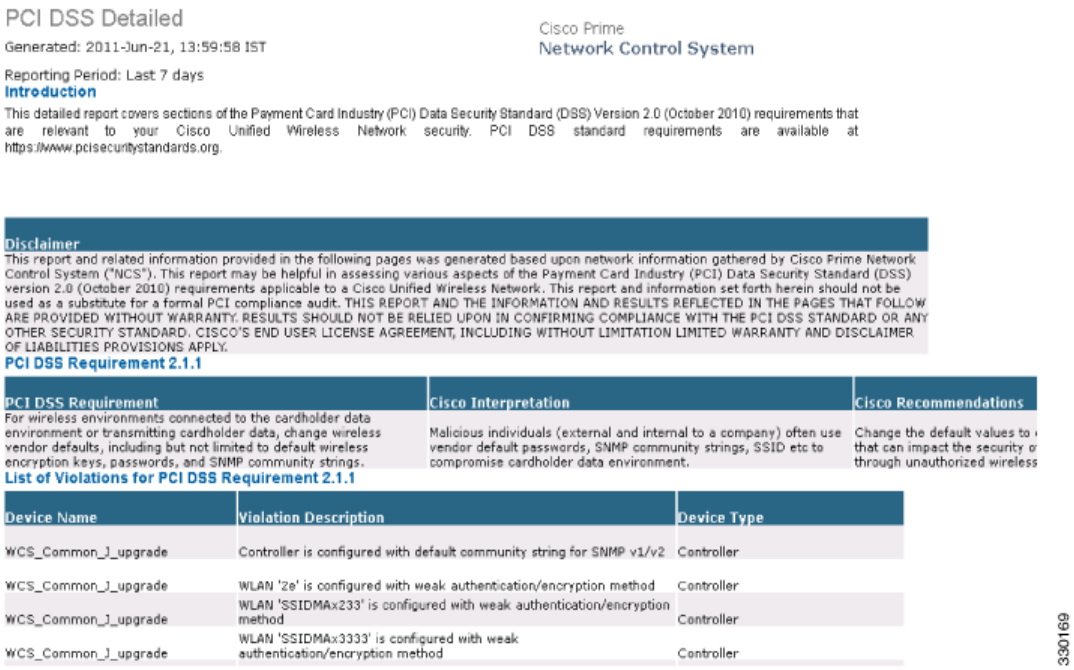
Click Customize to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

PCI DSS Detailed Report Results

The following are the results for a PCI DSS Detailed Report (see Figure 14-23):

Figure 14-23 PCI DSS Detailed Report



PCI DSS Detailed

Generated: 2011-Jun-21, 13:59:58 IST

Cisco Prime
Network Control System

Reporting Period: Last 7 days

Introduction

This detailed report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 2.0 (October 2010) requirements that are relevant to your Cisco Unified Wireless Network security. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.

Disclaimer

This report and related information provided in the following pages was generated based upon network information gathered by Cisco Prime Network Control System ("NCS"). This report may be helpful in assessing various aspects of the Payment Card Industry (PCI) Data Security Standard (DSS) version 2.0 (October 2010) requirements applicable to a Cisco Unified Wireless Network. This report and information set forth herein should not be used as a substitute for a formal PCI compliance audit. THIS REPORT AND THE INFORMATION AND RESULTS REFLECTED IN THE PAGES THAT FOLLOW ARE PROVIDED WITHOUT WARRANTY. RESULTS SHOULD NOT BE RELIED UPON IN CONFIRMING COMPLIANCE WITH THE PCI DSS STANDARD OR ANY OTHER SECURITY STANDARD. CISCO'S END USER LICENSE AGREEMENT, INCLUDING WITHOUT LIMITATION LIMITED WARRANTY AND DISCLAIMER OF LIABILITIES PROVISIONS APPLY.

PCI DSS Requirement 2.1.1

PCI DSS Requirement	Cisco Interpretation	Cisco Recommendations
For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Malicious individuals (external and internal to a company) often use vendor default passwords, SNMP community strings, SSID etc to compromise cardholder data environment.	Change the default values to that can impact the security o through unauthorized wireless

List of Violations for PCI DSS Requirement 2.1.1

Device Name	Violation Description	Device Type
WCS_Common_1_upgrade	Controller is configured with default community string for SNMP v1/v2	Controller
WCS_Common_1_upgrade	WLAN '2e' is configured with weak authentication/encryption method	Controller
WCS_Common_1_upgrade	WLAN 'SSIDMAx233' is configured with weak authentication/encryption method	Controller
WCS_Common_1_upgrade	WLAN 'SSIDMAx3333' is configured with weak authentication/encryption method	Controller

330169

PCI DSS Summary

This report displays a summarized PCI Data Security Standard (DSS) version 2.0 requirements that are relevant to your wireless network security.

Click **PCI DSS Summary** from the Report Launch Pad to open the PCI DSS Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the PCI DSS Summary Reports page. See the "Configuring a PCI DSS Summary Report" section on page 14-74 and the "PCI DSS Summary Report Results" section on page 14-75 for more information.

Configuring a PCI DSS Summary Report

This section describes how to configure a PCI DSS Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click Customize to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

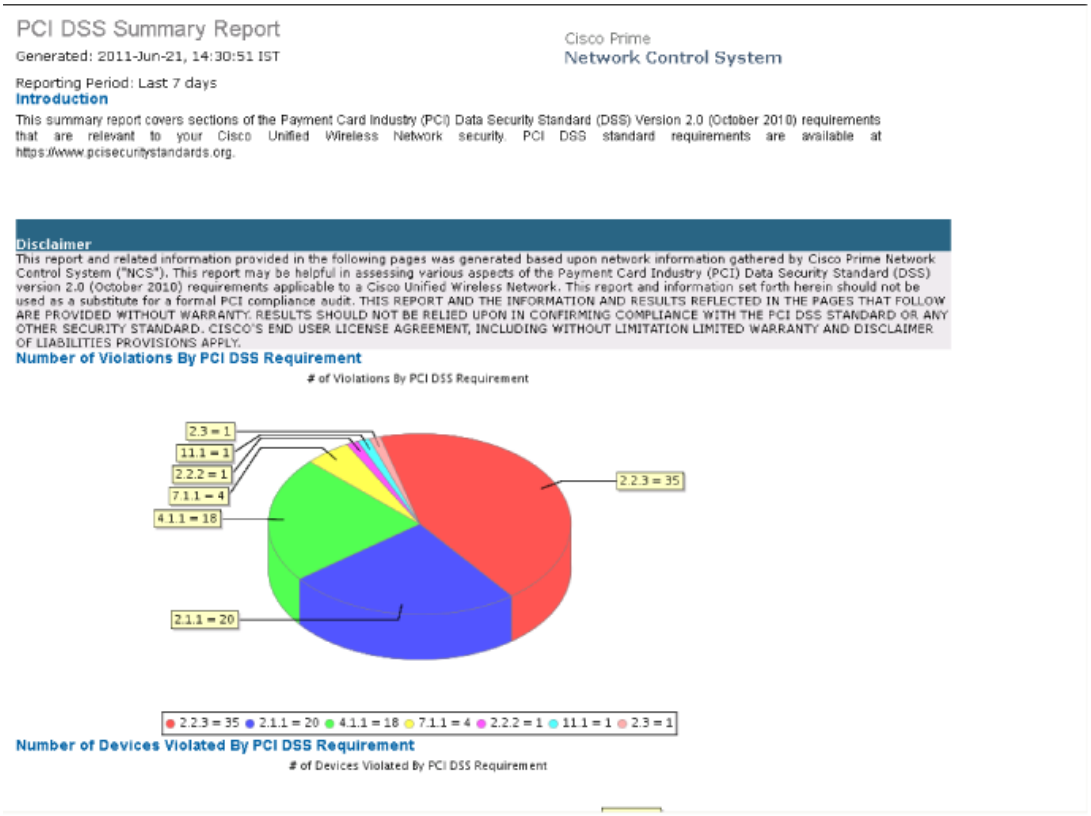
Note Fixed columns appear in blue font and cannot be moved to Available Columns.

PCI DSS Summary Report Results

The results of PCI DSS Summary Report contains the following information (see Figure 14-24 for a snippet):

- Number of Violations By PCI DSS Requirement
- Number of Devices Violated By PCI DSS Requirement
- Summary By PCI DSS Requirement
- Summary By Devices
- List of Violations

Figure 14-24 PCI DSS Summary Report



ContextAware Reports

This section lists and describes the various ContextAware reports that you can generate through the NCS Reports Launch Pad.

To generate a ContextAware report, under the ContextAware section, click **New** next to a type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

You can create the following ContextAware Reports:

Client Location History

This report displays Location history of a wireless client detected by an MSE.

This section consists of the following topics:

Configuring a Client Location History

This section describes how to configure a Client Location History report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Client MAC address.
- Report Criteria—Click **Edit** and enter a valid MAC address as the filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

Or

– Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Client Location History Results

The results of the Client Location History Report contains the following information:

- Last Located—The place at which the client was last located.
- Client Location—The current position of the client.
- MSE—The name of the MSE to which the client is associated with.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It could be either Probing.
- IP Address—The IP address of the client.
- AP MAC Address—The MAC address of the associated access point.
- Authenticated—Whether authenticated or not. This could be either Yes or No.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.

Client Location Tracking

This report displays wireless clients and their locations detected by the MSEs based on your filtering criteria.

This section consists of the following topics:

Configuring a Client Location Tracking

This section describes how to configure a Client Location Tracking report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Client Location Tracking Results

The results of the Client Location Tracking Report contains the following information:

- Last Located—The place where the client was last located.
- MAC Address—The MAC address of the client.

- Client Location—The current location of the client.
- MSE—The name of the MSE to which the client is associated with.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It could be either Probing.
- IP Address—The IP address of the client.
- SSID—The SSID used by the client
- Protocol—The protocol used to retrieve the information from the client.

Guest Location Tracking

This report displays Guest clients and their locations detected by the MSEs based on your filtering criteria.

This section consists of the following topics:

- Configuring a Guest Location Tracking, page 14-80
- Guest Location Tracking Results, page 14-81

Configuring a Guest Location Tracking

This section describes how to configure a Guest Location Tracking report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Guest Location Tracking Results

The results of the Guest Location Tracking Report contains the following information:

- Last Located—The place where the guest client was last located.
- Guest Username—The login name of the guest client user.
- MAC Address—The MAC address of the guest client.
- Guest Location—The current location of the guest client.
- MSE—The name of the MSE to which the guest client is associated with.
- Detecting Controllers—The IP address of the detecting controller.
- IP Address—The IP address of the guest client.
- AP MAC Address—The MAC address of the access point to which the guest client is associated with.
- SSID—The SSID used by the guest clients.
- Protocol—The protocol used to retrieve the information from the guest client.

Location Notifications

This report displays Context Aware Notifications generated by MSEs.

This section consists of the following topics:

Configuring a Location Notification

This section describes how to configure a Location Notification report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Missing Device Notifications by MSE
  - Missing Device Notifications by Floor Area
  - Missing Device Notifications by Outdoor Area
  - Device In/Out Notifications by MSE
  - Device In/Out Notifications by Floor Area
  - Device In/Out Notifications by Outdoor Area
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Device Type
  - All
  - Client
  - Tag
  - Rogue Client
  - Rogue AP
  - Interferer
- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Location Notification Results

The results of Location Notification Report contains the following information:

- Last Seen—The date and time when the device was last located.
- MAC Address—The MAC address of the device.
- Device Type—The type of the device.
- Asset Name—The name of the asset.
- Asset Group—The name of the asset group.
- Asset Category—The name of the asset category.
- Map Location—The map location where the device was located.
- serverName—The name of the server that sends the ContextAware notifications.

Rogue AP Location Tracking

This report displays Rogue APs and their locations detected by the MSEs based on your filtering criteria.

This section consists of the following topics:

- Configuring a Rogue AP Location Tracking, page 14-83
- Rogue AP Location Tracking Results, page 14-84

Configuring a Rogue AP Location Tracking

This section describes how to configure a Rogue AP Location Tracking report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

Or

– Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Rogue AP Location Tracking Results

The results of the Rogue AP Location Tracking Report contains the following information:

- Last Located—The place where the rogue access point was last located.
- MAC Address—The MAC address of the rogue access point.
- Rogue AP Location—The current location of the rogue access point.
- MSE—The name of the MSE to which the rogue access point is associated with.
- State—The state of the location tracking. This could be either Alert or Pending.

Rogue Client Location Tracking

This report displays Rogue Client APs and their locations detected by the MSEs based on your filtering criteria.

This section consists of the following topics:

Configuring a Rogue Client Location Tracking

This section describes how to configure a Rogue Client Location Tracking report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.

- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Rogue Client Location Tracking Results

The results of Rogue Client Location Tracking Report contains the following information:

- Last Located—The place where the client was last located.
- MAC Address—The MAC address of the rogue client.
- Rogue Client Location—The current location of the rogue client.
- MSE—The name of the MSE to which the rogue client is associated with.
- Rogue AP—The rogue access point to which the rogue client is associated with.
- Detecting Controllers—The IP address of the detecting controller.
- State—The state of the location tracking. This could be either Alert or Pending.

Tag Location History

This report displays Location history of a tag detected by an MSE.

This section consists of the following topics:

Configuring a Tag Location History

This section describes how to configure a Tag Location History report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Tag MAC address.
- Report Criteria—Click **Edit** and enter a valid Tag MAC address as the filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Tag Location History Results

The results of Tag Location History Report contains the following information:

- Last Located—The place at which the tag was last located.
- Tag Location—The current location of the tag.
- MSE—The name of the MSE to which this client is associated with.
- Detecting Controller—The IP address of the detecting controller.
- Vendor—The name of the vendor for the client.
- Battery Status—The battery status of the client.

Tag Location Tracking

This report displays tags and their locations detected by the MSEs based on your filtering criteria.

This section consists of the following topics:

- Configuring a Tag Location Tracking, page 14-87
- Tag Location Tracking Results, page 14-88

Configuring a Tag Location Tracking

This section describes how to configure a Tag Location Tracking report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Tag Location Tracking Results

The results of the Tag Location Tracking Report contains the following information:

- Last Located—The place at which the tag was last located.
- Tag Location—The current location of the tag.
- MSE—The name of the MSE to which this client is associated with.
- Detecting Controller—The IP address of the detecting controller.
- Vendor—The name of the tag vendor.
- Battery Status—The status of the battery of that tag.

Device Reports

Click **New** for a Device Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

You can create the following device reports:

- AP Image Predownload
- AP Profile Status
- AP Summary
- Busiest APs
- CPU Utilization
- Detailed Switch Inventory
- Identity Capability

- Inventory
- Memory Utilization
- Switch Interface Utilization
- Uptime
- Utilization

AP Image Predownload

This report displays scheduled download software task status.

Click **AP Image Predownload** from the Report Launch Pad to open the AP Image Predownload page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the AP Image Predownload Reports page. See the "Configuring an AP Image Predownload Report" section on page 14-89 and the "AP Image Predownload Report Results" section on page 14-90 for more information.

Configuring an AP Image Predownload Report

This section describes how to configure a AP Image Predownload report.

Settings

The following settings can be configured for a AP Image Predownload report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose specific devices.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.

Note In the Report Criteria page, you can choose **All Access Points** or **All OfficeExtend Access Points**.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Mandatory columns are displayed in blue font and cannot be moved to Available Columns. AP Name, Primary Image, Backup Image, Predownload Version, and Predownload Status are mandatory columns for the AP Image Predownload report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

AP Image Predownload Report Results

The following are potential results for an AP Image Predownload report, depending on how the report is customized:

- AP Name—Access point name.
- Primary Image—Current Primary Image present in the AP.
- Backup Image—Current Backup Image present in the AP.
- Predownload Version—The image version that is currently downloading to the AP from the controller as part of the predownload process.
- Predownload Status—The current status of the image download as part of the predownload process.
- MAC Address—MAC Address of the AP.
- Controller IP Address—IP address of the controller to which the access point is associated.

AP Profile Status

This report displays access point load, noise, interference, and coverage profile status.

Click **AP Profile Status** from the Report Launch Pad to open the AP Profile Status Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the AP Profile Status Reports page. See the "Configuring an AP Profile Report" section on page 14-91 and the "AP Profile Status Report Results" section on page 14-92 for more information.

Configuring an AP Profile Report

This section describes how to configure a AP Profile report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose specific devices.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.

Note In the Reports Criteria page, you can choose **All Access Points** or All OfficeExtend Access Points.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

AP Profile Status report results include:

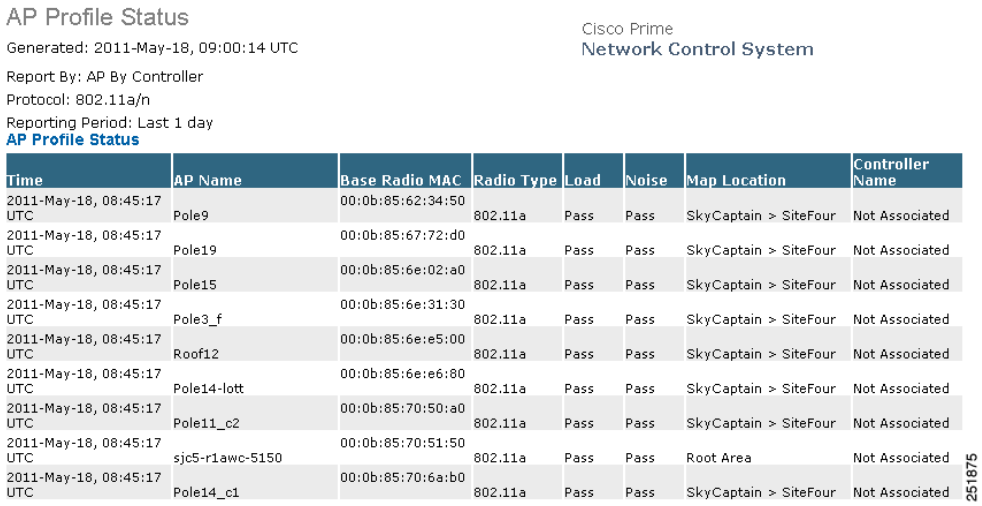
- Time—The date and time at which AP Profile Status is collected.
- AP Name—The access point name.
- AP MAC address—The MAC address of the access point.
- Radio Type—802.11a/n or 802.11b/g/n.
- Load—*True* if the load level exceeds a threshold level, otherwise *false*.
- Noise—*True* if the noise level exceeds a threshold level, otherwise *false*.
- Controller Name—The controller to which the access point is associated.
- Interference—*True* if the interference level exceeds a threshold level, otherwise *false*.
- Coverage—*True* if the coverage level exceeds a threshold level, otherwise *false*.
- Controller IP Address—The IP address of the controller to which the access point is associated.

AP Profile Status Report Results

The following are potential results for an AP Profile Status report, depending on how the report is customized (see Figure 14-25):

- Time (mandatory column)—The date and time at which AP Profile Status is collected.
- AP Name (mandatory column)—Access point name.
- AP MAC address—MAC address of the access point.
- Radio Type—802.11a/n or 802.11b/g/n.
- Load—Pass or Fail. Indicates whether or not the load level exceeds a threshold level.
- Noise—Pass or Fail. Indicates whether or not the noise level exceeds a threshold level.
- Interference—Pass or Fail. Indicates whether or not the interference level exceeds a threshold level.
- Coverage—Pass or Fail. Indicates whether or not the coverage level exceeds a threshold level.
- Controller Name—Name of the controller to which the access point is associated.
- Controller IP Address—IP address of the controller to which the access point is associated.

Figure 14-25 AP Profile Status Report Results



AP Profile Status

Generated: 2011-May-18, 09:00:14 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 1 day

Cisco Prime
Network Control System

AP Profile Status

Time	AP Name	Base Radio MAC	Radio Type	Load	Noise	Map Location	Controller Name
2011-May-18, 08:45:17 UTC	Pole9	00:0b:85:62:34:50	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole19	00:0b:85:67:72:d0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole15	00:0b:85:6e:02:a0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole3_f	00:0b:85:6e:31:30	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Roof12	00:0b:85:6e:e5:00	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole14-lott	00:0b:85:6e:e6:80	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole11_c2	00:0b:85:70:50:a0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	sjc5-r1awc-5150	00:0b:85:70:51:50	802.11a	Pass	Pass	Root Area	Not Associated
2011-May-18, 08:45:17 UTC	Pole14_c1	00:0b:85:70:6a:b0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated

251875

Busiest APs

This report displays the access points with the highest total usage (transmitting, receiving, and channel utilization) on your wireless network.

Click **Busiest APs** from the Report Launch Pad to open the Busiest APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Busiest APs Reports page. See the "Configuring a Busiest APs Report" section on page 14-93 and the "Configuring a Busiest APs Report" section on page 14-93 for more information.

Configuring a Busiest APs Report

This section describes how to configure a Busiest APs report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Protocol—Choose **802.11 a/n** or **802.11 b/g/n** from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Busiest APs report results include:

- AP Name—The access point name.
- Radio Type
- Rx Utilization (%)—The percentage of time that the access point receiver is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Tx Utilization (%)—The percentage of time that the access point transmitter is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Channel Utilization (%)—The percentage of time that an access point channel is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Controller Name
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller IP Address

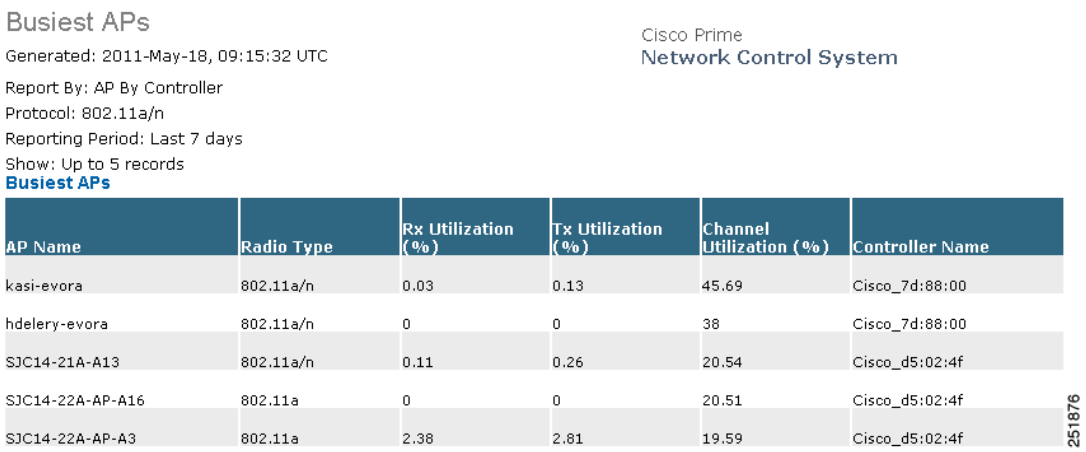
Busiest APs Report Results

The following are potential results for a Busiest APs report, depending on how the report is customized (see Figure 14-26):

- AP Name (mandatory column)
- Radio Type—802.11a/n or 802.11b/g/n.
- Rx Utilization (%)—The percentage of time the access point receiver is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
- Tx Utilization (%)—This is the percentage of time the access point transmitter is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.

- Channel Utilization (%)—This is the percentage of time an access point channel is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
- Controller Name and IP Address
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.

Figure 14-26 Busiest APs Report Results



Busiest APs

Generated: 2011-May-18, 09:15:32 UTC

Report By: AP By Controller
Protocol: 802.11a/n
Reporting Period: Last 7 days
Show: Up to 5 records

Cisco Prime
Network Control System

Busiest APs

AP Name	Radio Type	Rx Utilization (%)	Tx Utilization (%)	Channel Utilization (%)	Controller Name
kasi-evora	802.11a/n	0.03	0.13	45.69	Cisco_7d:88:00
hdelery-evora	802.11a/n	0	0	38	Cisco_7d:88:00
SJC14-21A-A13	802.11a/n	0.11	0.26	20.54	Cisco_d5:02:4f
SJC14-22A-AP-A16	802.11a	0	0	20.51	Cisco_d5:02:4f
SJC14-22A-AP-A3	802.11a	2.38	2.81	19.59	Cisco_d5:02:4f

251876

CPU Utilization

This report displays CPU utilization switch usage on your network.

Click **CPU Utilization** from the Report Launch Pad to open the CPU Utilization Report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the CPU Utilization Report page. See the "Configuring a CPU Utilization Report" section on page 14-95 for more information.

Configuring a CPU Utilization Report

This section describes how to configure a CPU Utilization report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type:
  - Switch CPU—
  - Top Switch CPU—
- Report By:
  - Switch IP

  - Device Name
- Report Criteria—Choose All Switches or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Detailed Switch Inventory

This report displays inventory information about the switches in your network.

Click **Detailed Switch Inventory** from the Report Launch Pad to open the Detailed Switch Inventory page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Detailed Switch Inventory page. See the "Configuring a Detailed Switch Inventory Report" section on page 14-96 for more information.

Configuring a Detailed Switch Inventory Report

This section describes how to configure a Detailed Switch Inventory report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report By:
  - Device IP
  - Device Name
- Report Criteria—Choose All Switches or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

The Detailed Switch Inventory report results include:

- Name
- Description
- Device IP Address
- Contact
- Location
- Sys Up Time

Identity Capability

This report displays the identity capability summary for the switches in your network.

Click **Identity Capability** from the Report Launch Pad to open the Identity Capability Report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Identity Capability Report page. See the "Configuring an Identity Capability Report" section on page 14-97 for more information.

Configuring an Identity Capability Report

This section describes how to configure a Identity Capability report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Memory Utilization

This report displays the memory utilization summary for the switches in your network.

Click **Memory Utilization** from the Report Launch Pad to open the report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Memory Utilization Report page. See the "Configuring a Memory Utilization Report" section on page 14-98 for more information.

Configuring a Memory Utilization Report

This section describes how to configure a Memory Utilization report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type:
  - Switch Memory Utilization
  - Top Switch Memory Utilization
- Report By:
  - Switch IP
  - Device Name
- Report Criteria—Choose All Switches or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Non-Primary Controller APs

This report displays the access points that are not connected to the configured primary controller.

Click **Non-Primary Controller APs** from the Report Launch Pad to open the report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Switch Interface Utilization page. See the "Configuring Switch Interface Utilization Report" section on page 14-100 for more information.

Configuring a Non-Primary Controller APs Report

This section describes how to configure a Non-Primary Controller APs report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Show—Enter the number of records that you want displayed in the report.

  Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

- Reporting Period
  - Select a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Non-Primary Controller APs Report Results

The following are potential results for a Busiest APs report, depending on how the report is customized:

- AP Name—The name of the access point
- Base Radio MAC—The MAC address of the base radio.
- Map Location—The location of the access point in the map.
- Associated Controller Name—The name of the controller to which the access point is associated with.
- Primary Controller Name—The name of the primary controller to which the access point is associated with.

Switch Interface Utilization

This report displays the devices with the highest utilization on your network.

Click **Switch Interface Utilization** from the Report Launch Pad to open the report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Switch Interface Utilization page. See the "Configuring Switch Interface Utilization Report" section on page 14-100 for more information.

Configuring Switch Interface Utilization Report

This section describes how to configure a Switch Interface Utilization report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type:
  - Top-N Rx Utilization
  - Top-N Tx Utilization
  - Bottom-N Rx Utilization
  - Bottom-N Tx Utilization
- Report By:

  - Device IP
  - Device Name
- Report Criteria—Choose All Switches or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

The Detailed Switch Inventory report results include:

- Device Name
- Device IP Address
- Interface Name
- Min Rx (%)
- Max Rx (%)
- Avg Rx (%)

Switch Interface Utilization Report Results

The following are potential results for a Switch Interface Utilization report, depending on how the report is customized:

- Device Name
- Device IP Address
- Interface Name
- Min Rx(%)
- Max Rx(%)
- Avg Rx(%)

AP Summary

This report displays a list of access points which are broadcasting SSID(s). This report allows you to filter the devices by RF group name, mobility group name, access point group name, SSID, location, and other statistics.

Note

- This report, by default, displays a list of access points that are broadcasting one or more SSIDs; the **All SSIDs** filter is chosen by default. Access points that are broadcasting no SSID are not displayed.
- The AP Summary report does not include Autonomous access points. For Autonomous access points, you need to run an Autonomous AP Summary report.

Click **AP Summary** from the Report Launch Pad to open the AP Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click New from the Report Launch Pad or from the AP Summary Reports page. See the "Configuring an AP Summary Report" section on page 14-102 and the "AP Summary Report Results" section on page 14-104 for more information.

Configuring an AP Summary Report

This section describes how to configure an AP Summary report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Floor Area—Choose **All Campuses > All Builders > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - OfficeExtend AP—Choose **Enable** from the Report Criteria page, or click **Edit** to choose **Enable** or **Disable**.
  - AP by Controller—Choose **All Controllers > All APs** from the Report Criteria page, or click **Edit** to choose specific devices.

- AP Group—Choose **All AP Groups** from the Report Criteria page, or click **Edit** to choose a specific access point group.
- RF Group—Choose **All RF Groups** from the Report Criteria page, or click **Edit** to choose a specific radio frequency group.
- AP Mode—Choose **All AP Modes** from the Report Criteria page, or click **Edit** to choose a specific access point mode.

Note This report only returns monitor mode access points if **Report by AP Mode** is selected. Reports run by any other **Report by** selection drop all monitor mode access points from the results.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- SSID—Choose the appropriate SSID from the list. You can choose *None* to show all access points with no SSIDs configured.

Note The SSID filter is tied to all the criteria in the Report By category. This limits the scope for getting a report of access points by any scope listed in the Report By criteria. For this report to be able to retrieve access points by any Report By criteria, the default selection of All SSIDs should be used.

Note Access points must be broadcasting SSID(s) in order to satisfy the "All SSID" default filter of the report.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

AP Summary report results include:

- AP Name—The access point name.
- Ethernet MAC Address
- Base radio MAC Address
- Model

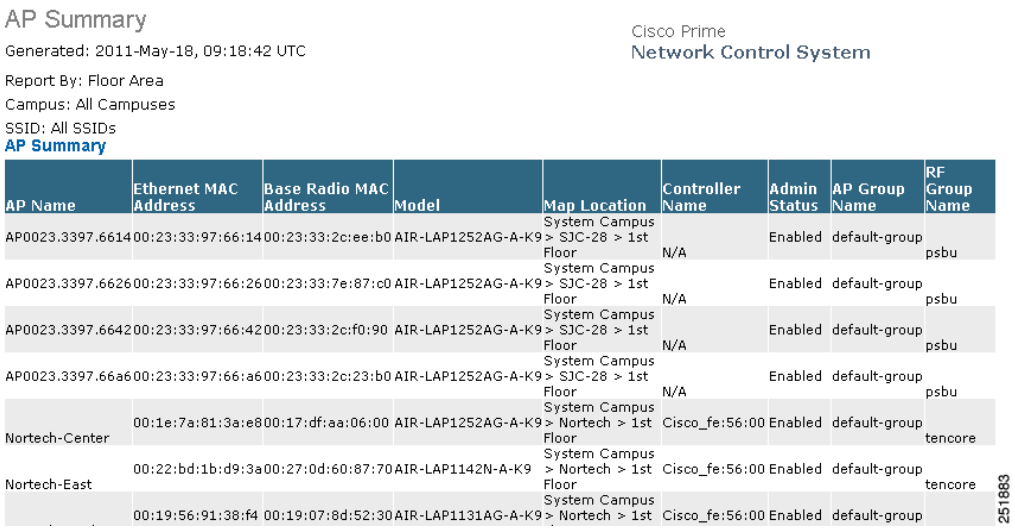
- Location
- Primary Controller
- Admin Status—Enable/Disable.
- AP group Name
- RF group Name
- Software Version
- Controller Version
- AP Mode—Local, Bridge, Rogue Detector, or H-REAP.
- Associated WLANs—Associated SSIDs.
- 802.11a/n and 802.11b/g/n Status—Up/Down.
- Serial Number
- AP Type—Indicates the type of access point (unified or autonomous).

AP Summary Report Results

The following are potential results for an AP Summary report, depending on how the report is customized (see Figure 14-27):

- AP Name (mandatory column)
- Ethernet MAC Address
- Base Radio MAC Address
- Model
- Location
- Primary Controller
- Admin Status—Enabled or disabled.
- AP Group Name
- RF Group Name
- Software Version
- Controller Name
- AP Mode—Access point mode including: Local, Bridge, Rogue Detector, or H-REAP
- Associated WLANs—Associated SSIDs
- 802.11a/n and 802.11b/g/n Status—Up or down
- Serial Number

Figure 14-27 AP Summary Report Results



AP Summary

Generated: 2011-May-18, 09:18:42 UTC

Report By: Floor Area

Campus: All Campuses

SSID: All SSIDs

Cisco Prime
Network Control System

AP Summary

AP Name	Ethernet MAC Address	Base Radio MAC Address	Model	Map Location	Controller Name	Admin Status	AP Group Name	RF Group Name
AP0023.3397.6614	00:23:33:97:66:14	00:23:33:2c:ee:b0	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
AP0023.3397.6626	00:23:33:97:66:26	00:23:33:7e:87:c0	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
AP0023.3397.6642	00:23:33:97:66:42	00:23:33:2c:f0:90	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
AP0023.3397.66a6	00:23:33:97:66:a6	00:23:33:2c:23:b0	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
Nortech-Center	00:1e:7a:81:3a:e8	00:17:df:aa:06:00	AIR-LAP1252AG-A-K9	System Campus > Nortech > 1st Floor	Cisco_fe:56:00	Enabled	default-group	tencore
Nortech-East	00:22:bd:1b:d9:3a	00:27:0d:60:87:70	AIR-LAP1142N-A-K9	System Campus > Nortech > 1st Floor	Cisco_fe:56:00	Enabled	default-group	tencore
	00:19:56:91:38:f4	00:19:07:8d:52:30	AIR-LAP1131AG-A-K9	System Campus > Nortech > 1st	Cisco_fe:56:00	Enabled	default-group	

251883

Inventory

This report allows you to generate inventory-related information for controllers, access points, and MSEs managed by NCS. This information includes hardware type and distribution, software distribution, CDP information, and other statistics.

Click **Inventory** from the Report Launch Pad to open the Inventory Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Inventory Reports page. See the "Configuring an Inventory Report" section on page 14-105 and the "Inventory Report Results" section on page 14-109 for more information.

Note The disassociated access points with model and serial number as **null** or **''** values will be filtered out from the AP Inventory reports.

Configuring an Inventory Report

This section describes how to configure an Inventory report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type—Choose **Combined Inventory**, **APs**, **Autonomous APs**, **Controllers**, or **MSEs** from the drop-down list.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note An Inventory report contains the following sections: Count of Controllers by Model, Count of Controllers by Software Version, Controller Inventory, Disassociated AP(s), Count of APs by Model, Count of APs by Software Version.
To customize report results for a particular section, choose the appropriate section from the Customizable Report drop-down list.

Available information for Count of Controllers by Model results contain the following:

- Model Name—The name of the model of the controller.
- Number of Controllers—The controller count for each model name.

Available information for Count of Controllers by Model results contain the following:

- Software Version—The software version of the controller.
- Number of Controllers—The controller count for each software version.

Available information for Controller Inventory results contain the following:

- Controller Name
- IP Address—The IP address of the controller.
- Location—The user-specified physical location of the controller.
- Interfaces—The names of the interfaces of the controller combined together by commas.
- Reachability Status—*Reachable* if the controller is currently manageable.
- Serial Number—The serial number of the controller.
- Model—The model name of the controller.
- Software Version—The software version of the controller.
- Mobility Group—The name of the mobility group to which the controller is assigned.
- RF Group—The name of the RF group to which the controller is assigned.
- Neighbor Name, Port, and Address—CDP neighbor information including the name, port, and IP address of the neighbor.
- Duplex—The duplex mode of the CDP neighbor interface.

Available information for Count of APs by Model results contain the following:

- Model Name—The name of the model of the access point.
- Number of APs—The access point count for each model name.

Available information for Count of APs by Software Version results contain the following:

- Software Version—The software version of the access point.
- Number of APs—The access point count for each software version.

Available information for AP Inventory results contain the following:

- AP Name—The access point name.
- Ethernet MAC Address—The Ethernet MAC address of the access point.
- IP Address—The IP address of the access point.
- Model—The name of the model of the access point.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name—The name of the controller to which the access point is associated.
- Base radio MAC Address—The MAC address of an access point.
- Software Version—The software version of an access point.
- Location—The user-specified physical location of an access point.
- Primary Controller—The name of the primary controller to which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or an access point is unable to find the controller with this name, it associates with the secondary controller.
- Secondary Controller—The name of the secondary controller to which the access point should associate if the primary controller is unavailable. If the primary and secondary controllers are not available, the access point associates with the tertiary controller.
- Tertiary Controller—The name of the tertiary controller to which the access point should associate if the primary and secondary controller is unavailable. If the primary, secondary, and tertiary switch are unavailable, it associates with the master controller.
- Admin Status—The admin status of the access point.
- AP Mode—The monitor only mode setting of the access point. The options are local, monitor, H-REAP, rogue detector, sniffer, and bridge.
- 802.11 a/n and 802.11 b/g/n Status—The operation state of the respective radio. The options are down, up, not associated, and unknown.
- Gateway—The gateway for the access point.
- Netmask—The netmask of the IP address of the access points.
- IOS and Boot Versions—The version of the IOS Cisco access point, and the major/minor boot version of the access point.
- Certificate Type—The access point certification type options are unknown, manufacture installed, self signed, or local significance.
- Serial Number—The serial number of the access point.
- Neighbor Name, Address, Port, and Advertised Version—The CDP neighbor name, IP address, port, and advertised version information of the access point.

Available information for Disassociated AP(s) results contain the following:

- AP Name—The access point name.
- Ethernet MAC Address—The Ethernet MAC address of the access point.

- IP Address—The IP address of the access point.
- Model—The name of the model of the access point.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name—The name of the controller to which the access point is associated.
- Base radio MAC Address—The MAC address of an access point.
- Software Version—The software version of an access point.
- Location—The user-specified physical location of an access point.
- Primary Controller—The name of the primary controller to which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or an access point is unable to find the controller with this name, it associates with the secondary controller.
- Secondary Controller—The name of the secondary controller to which the access point should associate if the primary controller is unavailable. If the primary and secondary controllers are not available, the access point associates with the tertiary controller.
- Tertiary Controller—The name of the tertiary controller to which the access point should associate if the primary and secondary controller is unavailable. If the primary, secondary, and tertiary switch are unavailable, it associates with the master controller.
- Admin Status—The admin status of the access point.
- AP Mode—The monitor only mode setting of the access point. The options are local, monitor, H-REAP, rogue detector, sniffer, and bridge.
- 802.11 a/n and 802.11 b/g/n Status—The operation state of the respective radio. The options are down, up, not associated, and unknown.
- Gateway—The gateway for the access point.
- Netmask—The netmask of the IP address of the access point.
- IOS and Boot Versions—The version of the IOS Cisco access point, and the major/minor boot version of the access point.
- Certificate Type—The access point certification type options are unknown, manufacture installed, self signed, or local significance.
- Serial Number—The serial number of the access point.
- Neighbor Name, Address, and Port—The CDP neighbor name, IP address, and port information of the access point.
- Duplex—CDP Neighbor interface duplex mode.
- AP Type—Indicates the type of access point (unified or autonomous).

Note The AP Inventory report displays only associated APs in the network.

Available information for Count of MSEs by Version results contain the following:

- Version—The MSE version.
- Number of MSEs—The count of both MSE and Location Servers.

Available information for MSEs results contain the following:

- Device Name—The name of the MSE or Location Server.

- IP Address
- Device Type
- HTTP/HTTPS Port
- HTTPS
- Version
- Start Time

Inventory Report Results

The following are potential results for an Inventory report, depending on how the report is customized (see Figure 14-28):

- Count of Controllers by Model results
  - Model Name (mandatory column)—Name of the model of the controller.
  - Number of Controllers (mandatory column)—Controller count for each model name.
- Count of Controllers by Model results
  - Software Version (mandatory column)—Software version of the controller.
  - Number of Controllers (mandatory column)—Controller count for each software version.
- Controller Inventory results
  - Controller Name (mandatory column)
  - IP Address—IP address of the controller.
  - Location—User specified physical location of the controller.
  - Interfaces—The names of the interfaces of the controller combined together by commas.
  - Reachability Status—Reachable if the controller is currently manageable.
  - Serial Number—Serial number of the controller.
  - Model—Model name of the controller.
  - Software Version—Software version of the controller.
  - Mobility Group—The name of the mobility group to which the controller is assigned.
  - RF Group—The name of the RF group to which the controller is assigned.
  - Neighbor Name, Port, and Address—CDP Neighbor information including the name, port and IP address of the neighbor.
  - Duplex—CDP Neighbor interface duplex mode.
- Count of APs by Model results
  - Model Name (mandatory column)—Name of the model of the access point.
  - Number of APs (mandatory column)—Access point count for each model name.
- Count of APs by Software Version results
  - Software Version (mandatory column)—Software version of the access point.
  - Number of APs (mandatory column)—Access point count for each software version.
- AP Inventory results
  - AP Name (mandatory column)

  - Ethernet MAC Address—Ethernet MAC address of the access point.
  - IP Address—IP address of the access point.
  - Model—Name of the model of the access point.
  - Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
  - Controller Name—Name of the controller to which the access point is associated.
  - Base Radio MAC Address—The MAC address of an access point base radio.
  - Software Version—The software version of an access point.
  - Location—User specified physical location of the access point.
  - Primary Controller—Name of the controller identified as the primary controller of the access point with which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or if the access point is not able to find the controller with this name, then it associates with the secondary controller.
  - Secondary Controller—Name of the controller identified as the secondary controller of the access point with which access point should associate if the primary controller is not available.

    If primary and secondary controllers are not available, then the access point associates with the tertiary controller.
  - Tertiary Controllers—Name of the controller identified as the tertiary controller of the access point with which access point should associate if the primary or secondary controllers are not available.

    If primary, secondary and tertiary switch are not available, then it associates with the master controller.
  - Admin Status—Administrative state of the access point.
  - AP Mode—Mode setting of the access point. Possible modes include: Local, Monitor, H-REAP, Rogue Detector, Sniffer, and Bridge.
  - 802.11 a/n and 802.11 b/g/n Status—Operation state of the respective radio. Possible statuses include Down, Up, Not Associated, and Unknown.
  - Gateway—The gateway for the access point.
  - Netmask—The netmask of the access point IP address.
  - IOS Version—IOS Version of the Cisco IOS access point.
  - Boot Version—Major and Minor boot version of the access point.
  - Certificate Type—Access point certification type. Possible types include: Unknown, Manufacture Installed, Self Signed, and Local Significance.
  - Serial Number—Serial number of the access point.
  - Neighbor Name, Address, Port, and Advertised Version—The access point CDP neighbor name, IP address, port, and advertised version information.

- Inventory results
  - AP Name (mandatory column)
  - Ethernet MAC Address
  - IP Address
  - Model

- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- 802.11 a/n and 802.11 b/g/n MAC Addresses
- Software Version
- Location
- Reachability Status
- 802.11 a/n and 802.11 b/g/n Status
- Serial Number

Figure 14-28 Inventory Report Results

Inventory Report

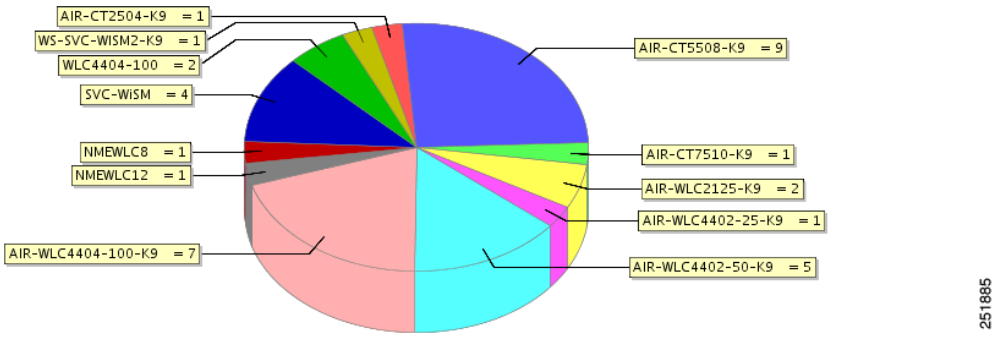
Generated: 2011-May-18, 09:21:10 UTC

Cisco Prime
Network Control System

Count of Controllers by Model

Model Name	Number of Controllers
AIR-CT2504-K9	1
AIR-CT5508-K9	9
AIR-CT7510-K9	1
AIR-WLC2125-K9	2
AIR-WLC4402-25-K9	1
AIR-WLC4402-50-K9	5
AIR-WLC4404-100-K9	7
NMEWLC12	1
NMEWLC8	1
SVC-WiSM	4
WLC4404-100	2
WS-SVC-WISM2-K9	1

Controllers by Model



Uptime

This report displays the access point uptime, the LWAPP uptime, and the LWAPP join time.

Click **Uptime** from the Report Launch Pad to open the Uptime Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Uptime Reports page. See the "Configuring an Uptime Report" section on page 14-112 and the "Configuring an Uptime Report" section on page 14-112 for more information.

Configuring an Uptime Report

This section describes how to configure an AP Image Predownload report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Uptime report results contain the following:

- AP Name—The access point name.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- AP Uptime—The time duration since the last access point reboot.
- LWAPP Uptime—The time duration since the last access point joined the controller.
- LWAPP Join Taken Time—The time it took for the access point to join the controller. This value could be significant in Mesh environments.

Uptime Report Results

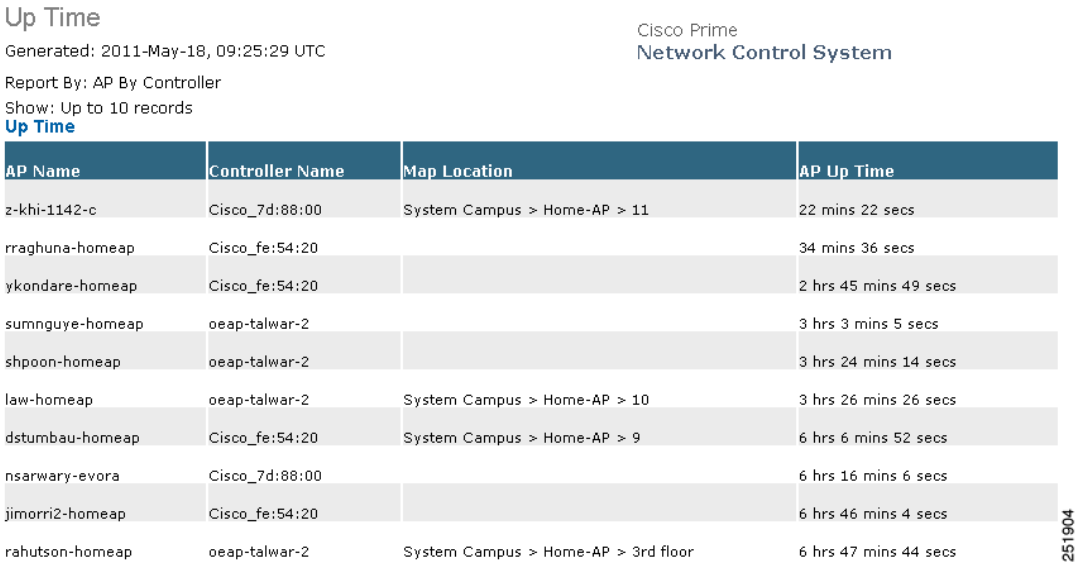
The following are potential results for an Uptime report, depending on how the report is customized (see Figure 14-29):

- AP Name

- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- AP Uptime—The length of time since the access point last rebooted.
- LWAPP Uptime—The length of time since the access point last joined the controller.
- LWAPP Join Taken Time—The amount of time the access point took to join the controller.

Note This could be a significant value in mesh environments.

Figure 14-29 Uptime Report Results



Up Time

Generated: 2011-May-18, 09:25:29 UTC

Report By: AP By Controller

Show: Up to 10 records

Cisco Prime
Network Control System

Up Time

AP Name	Controller Name	Map Location	AP Up Time
z-khi-1142-c	Cisco_7d:88:00	System Campus > Home-AP > 11	22 mins 22 secs
rraghuna-homeap	Cisco_fe:54:20		34 mins 36 secs
ykondare-homeap	Cisco_fe:54:20		2 hrs 45 mins 49 secs
sumnguye-homeap	oeap-talwar-2		3 hrs 3 mins 5 secs
shpoon-homeap	oeap-talwar-2		3 hrs 24 mins 14 secs
law-homeap	oeap-talwar-2	System Campus > Home-AP > 10	3 hrs 26 mins 26 secs
dstumbau-homeap	Cisco_fe:54:20	System Campus > Home-AP > 9	6 hrs 6 mins 52 secs
nsarwary-evora	Cisco_7d:88:00		6 hrs 16 mins 6 secs
jimorri2-homeap	Cisco_fe:54:20		6 hrs 46 mins 4 secs
rahutson-homeap	oeap-talwar-2	System Campus > Home-AP > 3rd floor	6 hrs 47 mins 44 secs

251904

Utilization

This report displays the controller, AP, and MSE usage on your wireless network. These statistics (such as CPU usage, memory usage, link utilization, and radio utilization) can help identify current network performance and help with capacity planning for future scalability needs.

Click **Utilization** from the Report Launch Pad to open the Utilization Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Utilization Reports page. See the "Configuring a Utilization Report" section on page 14-113 and the "Utilization Report Results" section on page 14-115 for more information.

Configuring a Utilization Report

This section describes how to configure a Utilization report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type—Choose **Controllers**, **MSEs**, or **Radios** from the drop-down list.
- Report by (Report by options change depending on the report type chosen)
  - Controller—If the report type is Controllers, choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices. Depending on the report type selected, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 14-114.
  - MSEs—If the report type is MSEs, choose **All MSEs** from the Report Criteria page, or click **Edit** to choose specific devices. Depending on the report type selected, you receive MSE memory and CPU utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 14-114.
  - Radios—If the report type is Radio, choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices). Depending on the report type chosen, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 14-114.

Note In the Radios Report Criteria page, you can choose **All Access Points** or **All OfficeExtend Access Points**.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **802.11 a/n**, **802.11 b/g/n**, or both. This parameter only appears if the report type is Radios.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Radio, Controller, and MSE Utilization Results

Depending on the report type chosen, you receive either radio, controller, or MSE utilization results.

- Radio Utilization
  - Rx Utilization (%)—The percentage of time that the access point receiver is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
  - Tx Utilization (%)—The percentage of time the access point transmitter is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.

  - Channel Utilization (%)—The percentage of time an access point channel is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
- Controller Utilization
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.
  - Port Utilization—The percentage of (totalDeltaBits/bandwidth) on a port.
- MSE Utilization
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.

Schedule

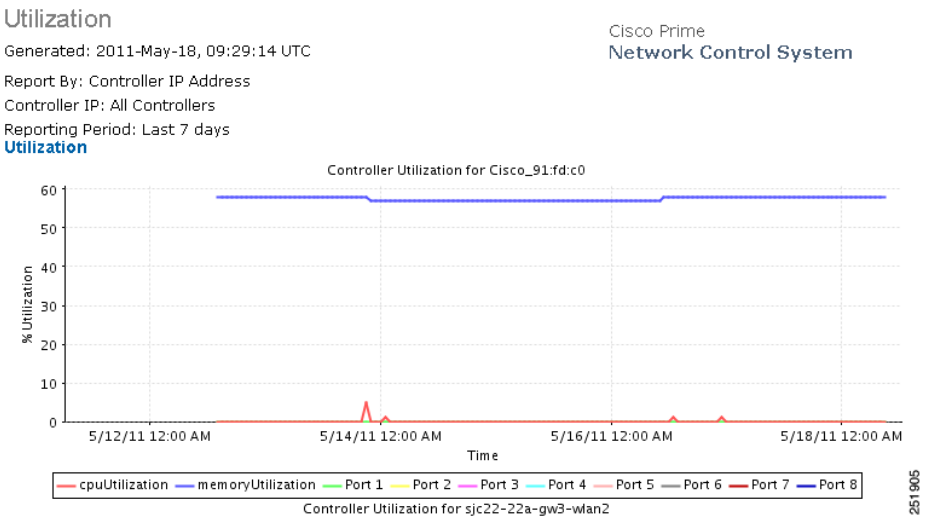
If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Utilization Report Results

The following are potential results for a Utilization report (see Figure 14-30):

- Controller results including CPU, memory, and port utilization.
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.
  - Port Utilization—The percentage of (totalDeltaBits/bandwidth) on a port.
- Radio results including channel, transmitting, and receiving utilization.
  - Channel Utilization—The percentage of time an AP channel is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
  - Rx Utilization—The percentage of time the AP receiver is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
  - Tx Utilization—The percentage of time the AP transmitter is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
- MSE results including memory utilization, CPU utilization, Context Aware Service statistics.
  - MSE CPU Utilization—The percentage of CPU utilization.
  - MSE Memory Utilization—The percentage of memory utilization.
  - Context Aware Service Statistics—Provides a graph of the count of the number of Clients, Tags, Rogue Client, Rogue APs, and Adhoc Rogue APs over a period of time.

Figure 14-30 Utilization Report Results



Guest Reports

You can create the following guest reports:

- Guest Accounts Status
- Guest Association
- Guest Count
- Guest User Sessions
- NCS Guest Operations

Guest Accounts Status

This report displays guest account status changes in chronological order. The report filters guest accounts by the guest user who created them. One example of a status change is Scheduled to Active to Expired.

Click **Guest Accounts Status** from the Report Launch Pad to open the Guest Accounts Status Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest Accounts Status Reports page. See the "Configuring a Guest Accounts Status Report" section on page 14-116 and the "Configuring a Guest Accounts Status Report" section on page 14-116 for more information.

Configuring a Guest Accounts Status Report

This section describes how to configure an Accounts Status report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - NCS User—Choose **All NCS Users** from the Report Criteria page, or click **Edit** to choose a specific NCS user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Guest Account Status report results contain the following:

- Time
- Guest username
- Created by
- Status

Guest Account Status Report Results

The following are potential results for a Guest Account Status report, depending on how the report is customized:

- Time
- Guest Username
- Created by

- Status

Guest Association

This report displays when a guest client associated to and disassociated from a guest profile/SSID over a customizable period of time.

Click **Guest Association** from the Report Launch Pad to open the Guest Association Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest Association Reports page. See the "Configuring a Guest Accounts Status Report" section on page 14-116 and the "Configuring a Guest Accounts Status Report" section on page 14-116 for more information.

Configuring a Guest Association Report

This section describes how to configure a Guest Association report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Guest Profile—Choose **All Profiles** from the Report Criteria page, or click **Edit** to choose a specific profile.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Guest Association report results contain the following:

- Time
- Guest user
- Guest MAC address
- Controller IP Address
- AP MAC Address
- Login and Logout Times
- Guest IP address
- Bytes Received
- Bytes Sent

Guest Association Report Results

The following are potential results for a Guest Association report, depending on how the report is customized:

- Time
- Guest MAC address and username
- Device IP address
- Guest profile
- Status
- AP Name
- Guest IP address
- Session Duration
- Reason—Reason for the disassociation

Guest Count

This report displays the number of guest clients logged into the network per guest profile/SSID over a customizable period of time.

Click **Guest Count** from the Report Launch Pad to open the Guest Count Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest Count Reports page. See the "Configuring a Guest Count Report" section on page 14-119 and the "Guest Count Report Results" section on page 14-120 for more information.

Configuring a Guest Count Report

This section describes how to configure a Guest Count report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Guest Profile—Choose **All Profiles** from the Report Criteria page, or click **Edit** to choose a specific profile.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Guest Count Report Results

The Guest Count results contain the following information:

- Authenticated Guest Count—Indicates the number of authenticated guests for each specified guest profile and protocol during the specified period of time.

Guest User Sessions

This report displays historic session data for a guest user. The session data such as amount of data passed, login and logout time, guest IP address, and guest MAC address is available for one month by default. The data retention period can be configured from the Administration > Background Tasks page. This report can be generated for guest users who are associated to controllers running software version 5.2 or above.

Click **Guest User Sessions** from the Report Launch Pad to open the Guest User Sessions Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest User Sessions Reports page. See the "Configuring a Guest User Sessions Report" section on page 14-121 and the "Guest User Sessions Report Results" section on page 14-121 for more information.

Configuring a Guest User Sessions Report

This section describes how to configure a Guest User Sessions report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - Guest User—Choose **All Guest Users** from the Report Criteria page, or click **Edit** to choose a specific guest user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

Schedule

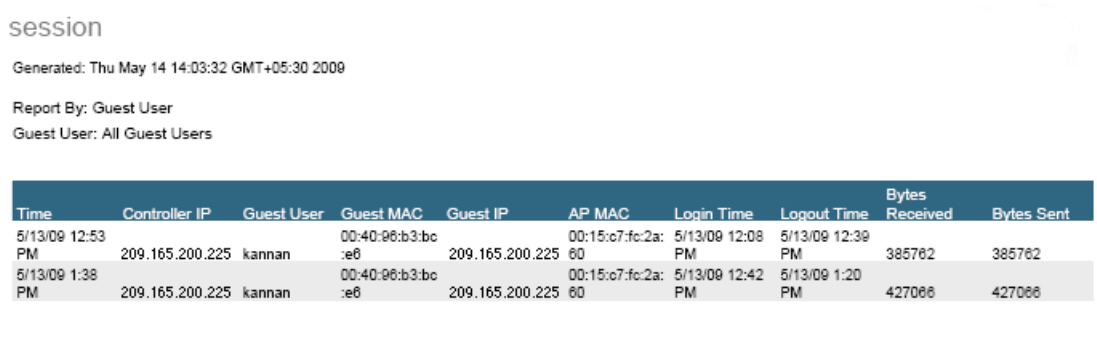
If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Guest User Sessions Report Results

The following are potential results for a Guest User Sessions report, depending on how the report is customized (see Figure 14-31):

- Time (mandatory column)
- Guest User (mandatory column)
- Guest User MAC Address (mandatory column)
- Controller IP Address
- Login Time
- Logout Time
- Guest IP Address
- Bytes Received
- Bytes Sent

Figure 14-31 Guest User Sessions Report Results


session

Generated: Thu May 14 14:03:32 GMT+05:30 2009

Report By: Guest User

Guest User: All Guest Users

Time	Controller IP	Guest User	Guest MAC	Guest IP	AP MAC	Login Time	Logout Time	Bytes Received	Bytes Sent
5/13/09 12:53 PM	209.165.200.225	kannan	00:40:96:b3:bc:e6	209.165.200.225	00:15:c7:fc:2a:60	5/13/09 12:08 PM	5/13/09 12:39 PM	385762	385762
5/13/09 1:38 PM	209.165.200.225	kannan	00:40:96:b3:bc:e6	209.165.200.225	00:15:c7:fc:2a:60	5/13/09 12:42 PM	5/13/09 1:20 PM	427066	427066

275957

NCS Guest Operations

This report displays all activities performed by one or all guests, such as creating, deleting, or updating guest user accounts. If a guest user is deleted from NCS, the report still shows an activity performed by the deleted guest user for up to one week after the activity occurred.

Click **NCS Guest Operations** from the Report Launch Pad to open the NCS Guest Operations Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the NCS Guest Operations Reports page. See the "Configuring a NCS Guest Operations Report" section on page 14-122 and the "NCS Guest Operation Report Results" section on page 14-123 for more information.

Configuring a NCS Guest Operations Report

This section describes how to configure a NCS Guest Operations report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - NCS User—Choose **All NCS Users** from the Report Criteria page, or click **Edit** to choose a specific user.

Note All NCS Users consists of the Lobby ambassador user groups and those Users who have done at least one guest account operation.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Guest Operation report results contain the following:

- Time
- Reason
- NCS User
- Guest User
- Operation
- Status

NCS Guest Operation Report Results

The following are potential results for a NCS Guest Operations report, depending on how the report is customized:

- Time
- NCS User
- Guest User
- Operation
- Status
- Reason

Identity Services Engine Reports

Cisco ISE 1.0 is a consolidated policy-based access control system that is integrated into the NCS 1.0. ISE helps in the monitoring of endpoint security policy to deliver visibility into compliance based on real-time contextual information from the network, users, and devices across the entire wired and wireless access network.

The following Identity Services Engine reports could be generated using the NCS Report Launch pad:

- Posture Detail Assessment
- Endpoint Profiler Summary
- Top N Endpoint MAC Authentications
- Endpoint MAC Authentication Summary
- User Authentication Summary
- Top N User Authentications
- Radius Accounting
- Radius Authentication

Note

- You can view the ISE reports in the Report Launch pad only when an ISE is added to NCS.
- To run the ISE reports, you need to enable the Identity Search Engine permission flag in the NCS > Administration > AAA > Groups > Group Detail menu option for the Super User, Config User, Admin, and System Monitoring user groups.
- When you launch the ISE reports from NCS using Internet Explorer 8, the report does not appear properly. To view the reports properly, refresh the content area (not the browser) by right clicking on the report details and selecting Refresh this frame option.

For more information on these reports, see the Available Reports section of the Reporting chapter of the *Cisco Identity Services Engine User Guide, Release 1.0*:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Mesh Reports

This section consists of the following reports:

- Alternate Parent
- Link Stats
- Nodes
- Packet Stats
- Packet Error Statistics
- Packet Queue Statistics
- Stranded APs
- Worst Node Hops

Alternate Parent

This report displays the number of alternate parents with the same configured mesh group for each mesh access point. This report can be used to determine an access point capability to handle failures in the mesh path.

Click **Alternate Parent** from the Report Launch Pad to open the Alternate Parent Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Alternate Parent Reports page. See the "Configuring an Alternate Parent Report" section on page 14-125 and the "Alternate Parent Report Results" section on page 14-125 for more information.

Configuring an Alternate Parent Report

This section describes how to configure an Alternate Parent report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Alternate Parent report results contain the following:

- AP Name—The access point name.
- MAC address
- Parent AP name
- Number Alternate parents
- Parent MAC address

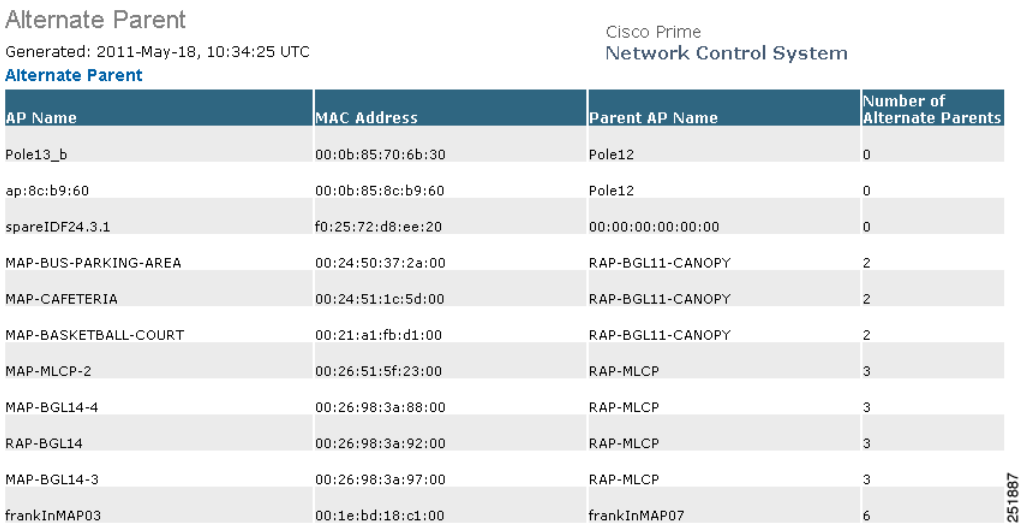
Alternate Parent Report Results

The following are potential results for an Alternate Parent report, depending on how the report is customized (see Figure 14-32):

- AP Name (mandatory column)
- MAC Address—The MAC address of the alternate parent.

- Parent AP Name and MAC Address
- Number of Alternate Parents

Figure 14-32 Alternate Parent Report Results



Alternate Parent

Generated: 2011-May-18, 10:34:25 UTC

Cisco Prime
Network Control System

Alternate Parent

AP Name	MAC Address	Parent AP Name	Number of Alternate Parents
Pole13_b	00:0b:85:70:6b:30	Pole12	0
ap:8c:b9:60	00:0b:85:8c:b9:60	Pole12	0
spareIDF24.3.1	f0:25:72:d8:ee:20	00:00:00:00:00:00	0
MAP-BUS-PARKING-AREA	00:24:50:37:2a:00	RAP-BGL11-CANOPY	2
MAP-CAFETERIA	00:24:51:1c:5d:00	RAP-BGL11-CANOPY	2
MAP-BASKETBALL-COURT	00:21:a1:fb:d1:00	RAP-BGL11-CANOPY	2
MAP-MLCP-2	00:26:51:5f:23:00	RAP-MLCP	3
MAP-BGL14-4	00:26:98:3a:88:00	RAP-MLCP	3
RAP-BGL14	00:26:98:3a:92:00	RAP-MLCP	3
MAP-BGL14-3	00:26:98:3a:97:00	RAP-MLCP	3
frankInMAP03	00:1e:bd:18:c1:00	frankInMAP07	6

251887

Link Stats

This report displays mesh link and node statistics such as parent access point, link SNR, packet error rate, parent changes, node hops, total transmit packets, mesh path, connected access points, mesh group, data rate, and channel. The mesh link and mesh node statistics can be run individually or combined.

Click **Link Stats** from the Report Launch Pad to open the Link Stats Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Link Stats Reports page. See the "Configuring a Link Stats Report" section on page 14-126 and the "Link Stats Report Results" section on page 14-127 for more information.

Configuring a Link Stats Report

This section describes how to configure a Link Stats report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type—Choose **Link Stats** or **Node Hops** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Link Stats report results contain the following:

- Time
- MAC address
- Parent MAC address
- AP Name—The access point name.
- Parent AP name
- Link SNR
- Packet Error Rate
- Parent changes
- Parent changes per minute
- Node hops
- Total Tx Packets
- Total Tx Packets per minute

Link Stats Report Results

The following are potential results for a Link Stats report, depending on how the report is customized (see Figure 14-33):

- Time (mandatory column)
- MAC Address (mandatory column)
- Parent MAC Address (mandatory column)
- AP Name
- Parent AP Name
- Link SNR
- Packet Error Rate—Packet error rate percentage = 1- (number of successfully transmitted packets/number of total packets transmitted)
- Parent Changes and Parent Changes per Minute
- Node hops—The number of hops between access points
- Total Tx Packets and Total Tx Packets per Minute

Figure 14-33 Link Stats Report Results

Link Stats

Generated: 2011-May-18, 16:54:25 UTC

Report By: AP By Controller

Reporting Period: Last 3 days

Cisco Prime
Network Control System

Link Stats

Time	MAC Address	Parent MAC Address	AP Name	Parent AP Name	Link SNR	Packet Error Rate
2011-May-15, 16:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	26	0.04
2011-May-15, 17:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 18:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 19:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	24	0.04
2011-May-15, 20:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 21:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 22:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	26	0.04
2011-May-15, 23:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-16, 00:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	26	0.04

251886

Nodes

This report displays mesh tree information for each mesh access point such as hop count, number of directly connected children, number of connected access points, and mesh path.

Click **Nodes** from the Report Launch Pad to open the Mesh Nodes Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Mesh Nodes Reports page. See the "Configuring a Nodes Report" section on page 14-128 and the "Configuring a Nodes Report" section on page 14-128 for more information.

Configuring a Nodes Report

This section describes how to configure a Nodes report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Node report results contain the following:

- MAC Address—The MAC address of the mesh access point.
- AP Name—The name of the mesh access point.
- Node Hops—The number of node hops for this mesh group.
- Children—The number of children for this access point.
- Connected APs—The number of access points connected to this access point.
- Mesh Path—The path of the mesh access point.
- Controller—The controller to which the mesh access point is associated.
- Mesh Role—Mesh access point (MAP) or Root access point (RAP).
- Mesh Group—The name of the mesh group to which this access point belongs.
- Data Rate—The data rate for this access point.
- Channel—The channel on which this access point is located.

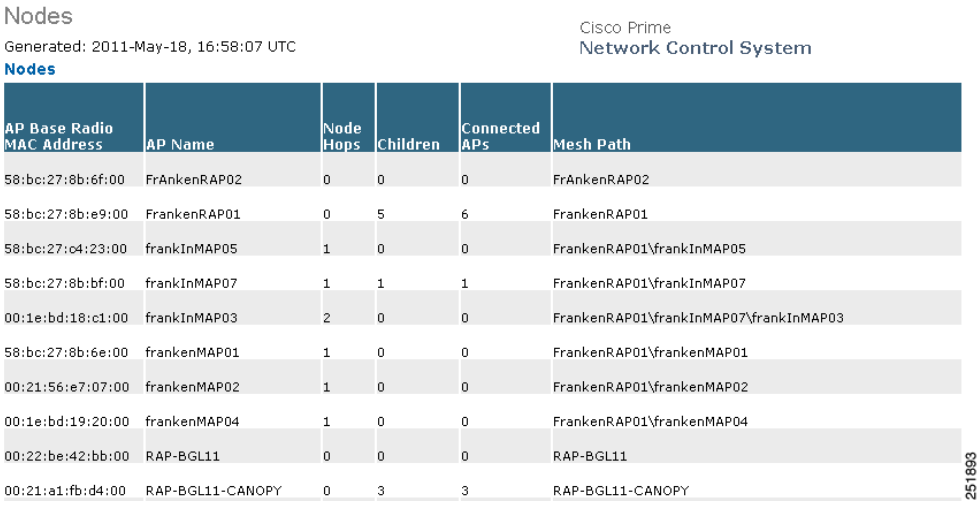
Nodes Report Results

The following are potential results for a Nodes report, depending on how the report is customized (see Figure 14-34):

- AP Name (mandatory column).
- AP MAC Address (mandatory column).
- Node Hops—The number of hops between access points.
- Children—The number of children for this access point.
- Connected APs—The number of access points connected to this access point.
- Mesh Path—The path of the mesh access point.
- Controller—The controller to which the mesh access point is associated.
- Mesh Role—Mesh access point (MAP) or Root access point (RAP).
- Mesh Group—The name of the mesh group to which this access point belongs.

- Data Rate—The data rate for this access point.
- Channel—The channel on which this access point is located.

Figure 14-34 Node Report Results



Nodes

Generated: 2011-May-18, 16:58:07 UTC

Cisco Prime
Network Control System

Nodes

AP Base Radio MAC Address	AP Name	Node Hops	Children	Connected APs	Mesh Path
58:bc:27:8b:6f:00	FrAnkenRAP02	0	0	0	FrAnkenRAP02
58:bc:27:8b:e9:00	FrankenRAP01	0	5	6	FrankenRAP01
58:bc:27:c4:23:00	frankInMAP05	1	0	0	FrankenRAP01\frankInMAP05
58:bc:27:8b:bf:00	frankInMAP07	1	1	1	FrankenRAP01\frankInMAP07
00:1e:bd:18:c1:00	frankInMAP03	2	0	0	FrankenRAP01\frankInMAP07\frankInMAP03
58:bc:27:8b:6e:00	frankenMAP01	1	0	0	FrankenRAP01\frankenMAP01
00:21:56:e7:07:00	frankenMAP02	1	0	0	FrankenRAP01\frankenMAP02
00:1e:bd:19:20:00	frankenMAP04	1	0	0	FrankenRAP01\frankenMAP04
00:22:be:42:bb:00	RAP-BGL11	0	0	0	RAP-BGL11
00:21:a1:fb:d4:00	RAP-BGL11-CANOPY	0	3	3	RAP-BGL11-CANOPY

251893

Packet Stats

This report displays the total number of packets transmitted, packets transmitted per minute, packet queue average, packet dropped count, packets dropped per minute, and errors for packets transmitted by neighbor access points. A report type can be chosen for each data type.

Click **Packet Stats** from the Report Launch Pad to open the Packet Stats Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Packet Stats Reports page. See the "Configuring a Packet Stats Report" section on page 14-130 and the "Packet Stats Report Results" section on page 14-131 for more information.

Configuring a Packet Stats Report

This section describes how to configure a Packet Stats report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Packet Stats** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Graph Type—Choose the type of graph you want displayed for these report results (Packet Counts or Packets Per Minute).
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

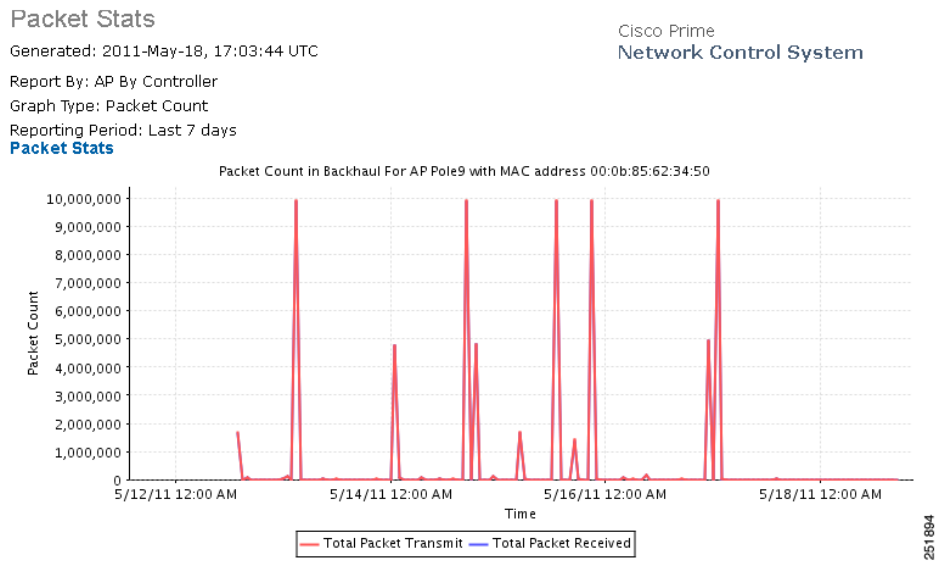
Packet Stats Report Results

The Packet Stats report generates a graph of packet queue statistics for each access point selected and for each report type selected. The graph types are Packet Queue Average, Packets Dropped Per Minute, and Packet Dropped Count.

The following are potential results for a Packet Stats report, depending on how the report is customized (see Figure 14-35):

- Packet Stats
  - Packet Count—Total packets transmitted and total packets received.
  - Packets per Minute—Total packets transmitted per minute and total packets received per minute.
- Packet Error Stats
  - Packet error rate percentages for all neighbor access points or for parent/children neighbor access points only.
- Packet Queue Stats
  - Packet Queue Average—Shows the average number of packets for each queue when the MIB was polled. Silver, gold, platinum, bronze, and management.
  - Packets Dropped Count—Contains the counter for the number of packets dropped.
  - Packets Dropped per Minute—Shows the number of packets dropped since the last sample divided by the number of minutes since the sample.

Figure 14-35 Packet Stats Report Results



Packet Error Statistics

This report notes the percentages of packet errors for packets transmitted by the neighbor mesh access point. The packet error rate percentage is 1 minus the number of successfully transmitted packets/numbers of total packets transmitted.

Configuring a Packet Error Statistics Report

This section describes how to configure a Packet Error Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Packet Error Stats** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Neighbor Type—Choose All Neighbors or Parent/Children Only.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

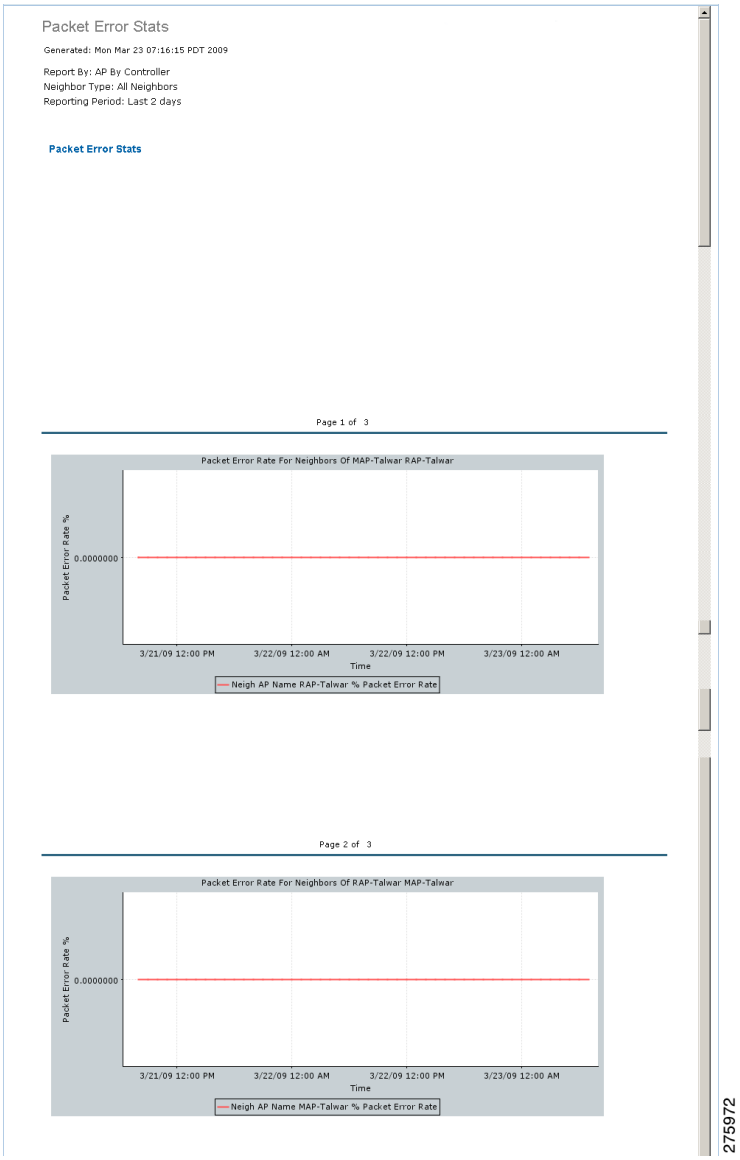
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Packet Error Statistics Report Results

The Packet Error Statistics report contains the following results (Figure 14-36):

Figure 14-36 Packet Error Statistics Report Results



Packet Queue Statistics

This report generates a graph of the total number of packets transmitted and the total number of packets successfully transmitted by the neighbor mesh access point.

Configuring a Packet Queue Statistics Report

This section describes how to configure a Packet Queue Statistics report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type—Choose **Packet Queue Stats** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Graph Type—Choose the type of graph you want displayed for these report results (**Packet Queue Average**, **Packets Dropped Count**, or **Packets Dropped Per Minute**).
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

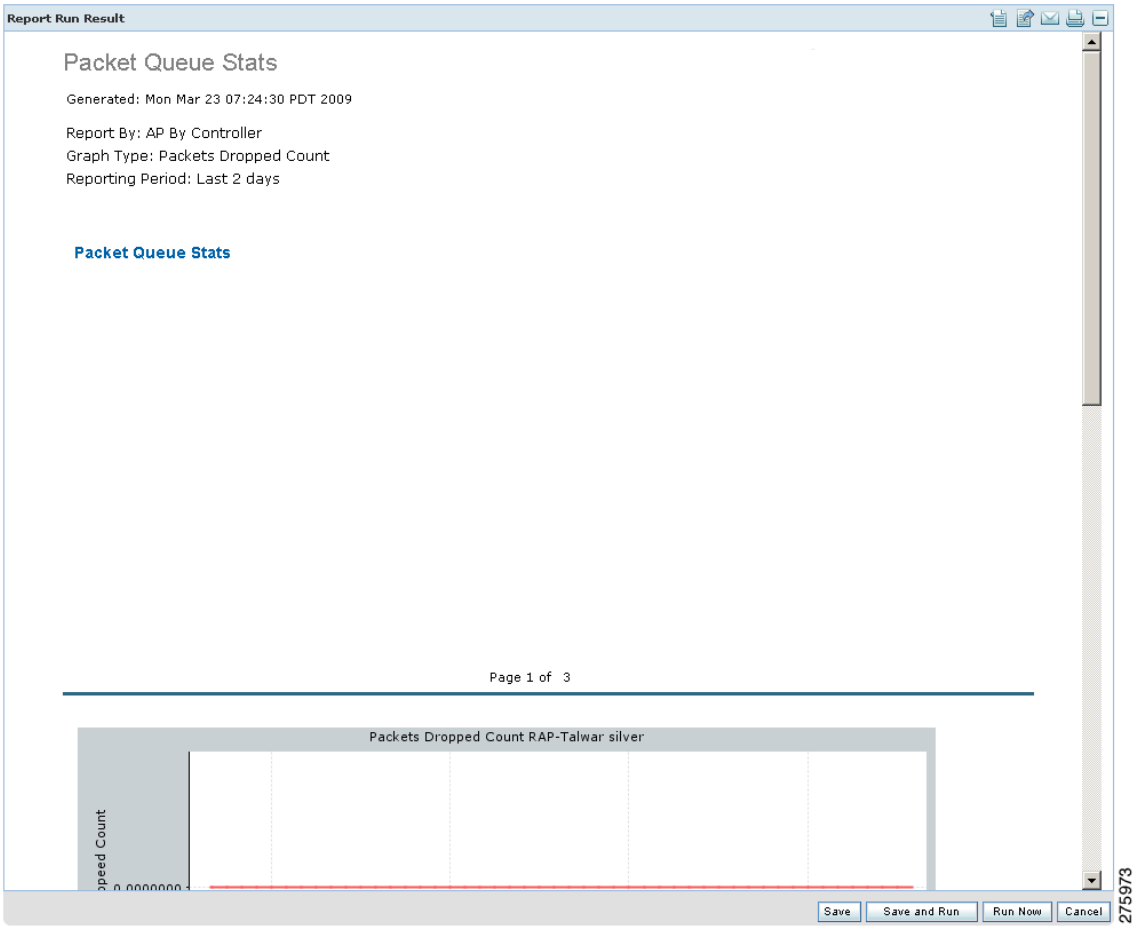
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Packet Queue Statistics Report Results

The Packet Queue Statistics report contains the following results (Figure 14-37):

Figure 14-37 Packet Queue Statistics Report Results



Stranded APs

This report displays access points that appear to be stranded. These access points might have joined a controller at one time and are no longer joined to a controller managed by NCS, or they might have never joined a controller managed by NCS.

Click **Stranded APs** from the Report Launch Pad to open the Stranded APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Stranded APs Reports page. See the "Configuring a Stranded APs Report" section on page 14-136 and the "Stranded APs Report Results" section on page 14-137 for more information.

Configuring a Stranded APs Report

This section describes how to configure a Stranded APs report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Stranded States—Choose **APs Managed by NCS** or **All**.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Link Stats report results contain the following:

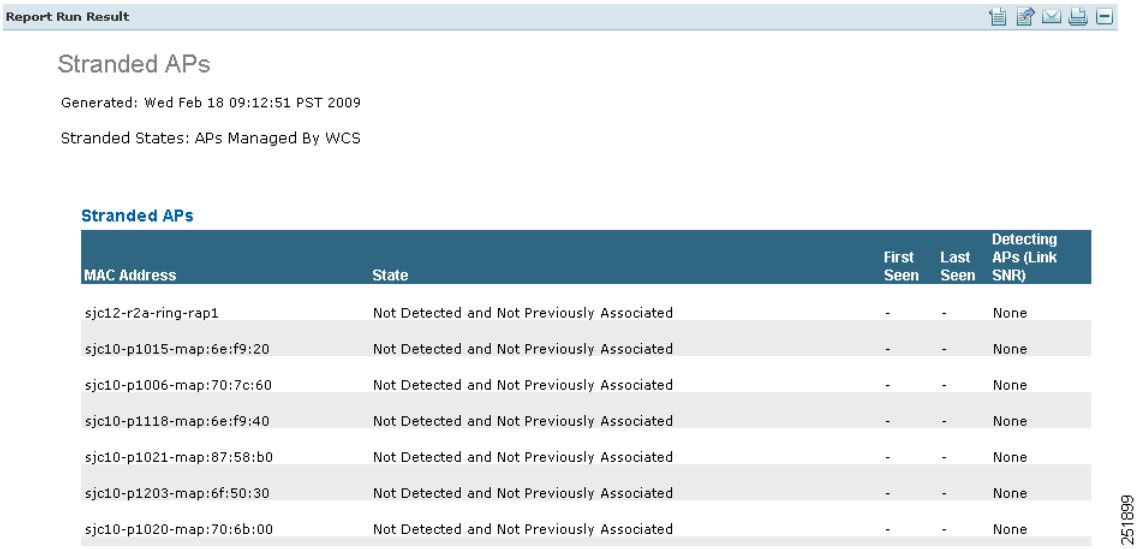
- MAC Address—The MAC address of the stranded access point.
- State—The state of the stranded access point (such as Not Detected and Not Previously Associated).
- First Seen—The date and time this access point was first detected.
- Last Seen—The date and time this access point was last seen.
- Detecting APs (Link SNR)—The access point(s) that detected this stranded access point.

Stranded APs Report Results

The following are potential results for a Stranded APs report, depending on how the report is customized (see Figure 14-38):

- MAC Address (mandatory column)—The MAC address of the stranded access point.
- State (mandatory column)—The state of the stranded access point (such as Not Detected and Not Previously Associated).
- First Seen—The date and time this access point was first detected.
- Last Seen—The date and time this access point was last seen.
- Detecting APs (Link SNR)—The access point(s) that detected this stranded access point.

Figure 14-38 Stranded APs Report Results



Report Run Result

Stranded APs

Generated: Wed Feb 18 09:12:51 PST 2009

Stranded States: APs Managed By WCS

Stranded APs

MAC Address	State	First Seen	Last Seen	Detecting APs (Link SNR)
sjc12-r2a-ring-rap1	Not Detected and Not Previously Associated	-	-	None
sjc10-p1015-map:6e:f9:20	Not Detected and Not Previously Associated	-	-	None
sjc10-p1006-map:70:7c:60	Not Detected and Not Previously Associated	-	-	None
sjc10-p1118-map:6e:f9:40	Not Detected and Not Previously Associated	-	-	None
sjc10-p1021-map:87:58:b0	Not Detected and Not Previously Associated	-	-	None
sjc10-p1203-map:6f:50:30	Not Detected and Not Previously Associated	-	-	None
sjc10-p1020-map:70:6b:00	Not Detected and Not Previously Associated	-	-	None

251899

Worst Node Hops

This report displays the worst node hops or backhaul SNR links for the specified reporting period. The information is displayed in both table and graph form. Report types include worst node hops, worst SNR links for all neighbors, and worst SNR links for parent/children only.

Click **Worst Node Hops** from the Report Launch Pad to open the Worst Node Hops Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Node Hops Reports page. See the "Configuring a Worst Node Hops Report" section on page 14-138 and the "Worst Node Hops Report Results" section on page 14-140 for more information.

Configuring a Worst Node Hops Report

This section describes how to configure a Worst Node Hops report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report Type—Choose **Worst Node Hops** or **Worst SNR Links** from the drop-down list.
- Report Type—When **Worst Node Hops** is chosen from the Report Type above, choose **Table Only** or **Table and Graph** to determine how the report results display.
- Neighbor Type—When **Worst SNR Links** is selected from the Report Type, choose **All Neighbors (Table Only)**, **Parent/Children Only (Table Only)**, **All Neighbors (Table and Graph)**, or **Parent/Children Only (Table and Graph)** to determine how the report results display.
- Reporting Period.

- Last—Select the **Last** radio button and a period of time from the drop-down list.
- From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note Worst Node Hops and Worst SNR Links reports are available in both table and graph reports. To customize report results for a particular section, choose the applicable section from the Customizable Report drop-down list.

Available information for Worst Node Hops report results contain the following:

- AP Name—The access point name.
- Node Hops—The number of node hops.
- MAC Address—The MAC address of the access point.
- Parent AP Name—The name of the parent access point.
- Parent MAC Address—The MAC address of the parent access point.
- Time (graph only)—The time of the node hop count.

Available information for Worst SNR Links report results contain the following:

- AP Name—The access point name.
- MAC Address—The MAC address of the access point.
- Neigh SNR—The neighbor signal-to-noise ratio.
- Neigh AP Name—The name of the neighbor access point.
- Neigh MAC Address—The MAC address of the neighbor access point.

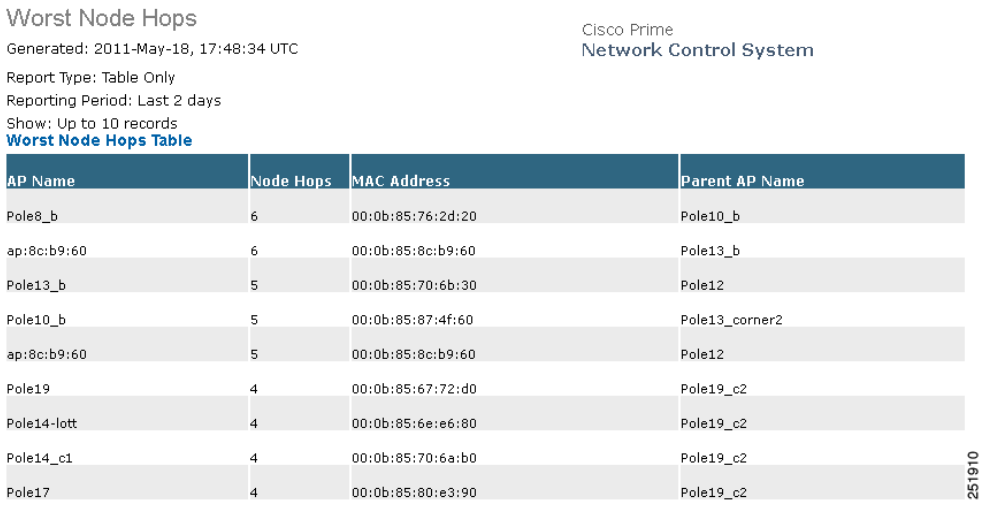
- Neigh Type—The neighbor type.
- Time (graph only)—The time of the current report statistics.

Worst Node Hops Report Results

The following are potential results for a Worst Node Hops report, depending on how the report is customized (see Figure 14-39):

- Worst Node Hops report results (table)
  - AP Name (mandatory column).
  - Node Hops (mandatory column)—The number of hops between access points.
  - MAC Address (mandatory column)—The MAC address of the access point.
  - Parent AP Name and MAC Address
- Worst Node Hops report results (graph)
  - Time (mandatory column)—The time of the node hop count.
  - MAC Address (mandatory column)—The MAC address of the access point.
  - Node Hops (mandatory column)—The number of hops between access points.
  - AP Name (mandatory column).
  - Parent AP Name and MAC Address.
- Worst SNR Links report results
  - AP Name (mandatory column).
  - MAC Address (mandatory column in graph report)—The MAC address of the access point.
  - Neighbor SNR (mandatory column).
  - Neighbor AP Name (mandatory column in graph report).
  - Neighbor MAC Address and Type.
  - Time (graph only)(mandatory column)—The time of the current report statistics.

Figure 14-39 Worst Node Hops Report Results



Network Summary

Click **New** for a Network Summary Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

The section contains the following Network Summary Reports:

- 802.11n Summary
- Executive Summary

802.11n Summary

This report displays a summary of 802.11n clients and client bandwidth usage for a customizable period of time.

Click **802.11n Summary** from the Report Launch Pad to open the 802.11n Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the 802.11n Summary Reports page. See the "Configuring an 802.11n Summary Report" section on page 14-141 and the "802.11n Summary Report Results" section on page 14-142 for more information.

Configuring an 802.11n Summary Report

This section describes how to configure an 802.11n Summary report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

802.11n Summary Report Results

The following information is displayed for the 802.11n Summary report:

- Number of access points per 802.11n band (pie graph)
- Utilization for 802.11n clients during the specified period of time (line graph)
- Number of associated clients for each protocols during the specified period of time (line graph)

Executive Summary

This report displays a quick view of your wireless network.

Click **Executive Summary** from the Report Launch Pad to open the Executive Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Executive Summary Reports page. See the "Configuring an Executive Summary Report" section on page 14-142 and the "Executive Summary Report Results" section on page 14-142 for more information.

Configuring an Executive Summary Report

This section describes how to configure an Executive Summary report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Executive Summary Report Results

The following information is displayed in the Executive Summary report (see Figure 14-40):

- Number of network devices including access points, controllers, and MSEs.
- Number of LWAPP versus autonomous access points (pie graph).
- Number of associated client in the network during the specified period of time (line graph).

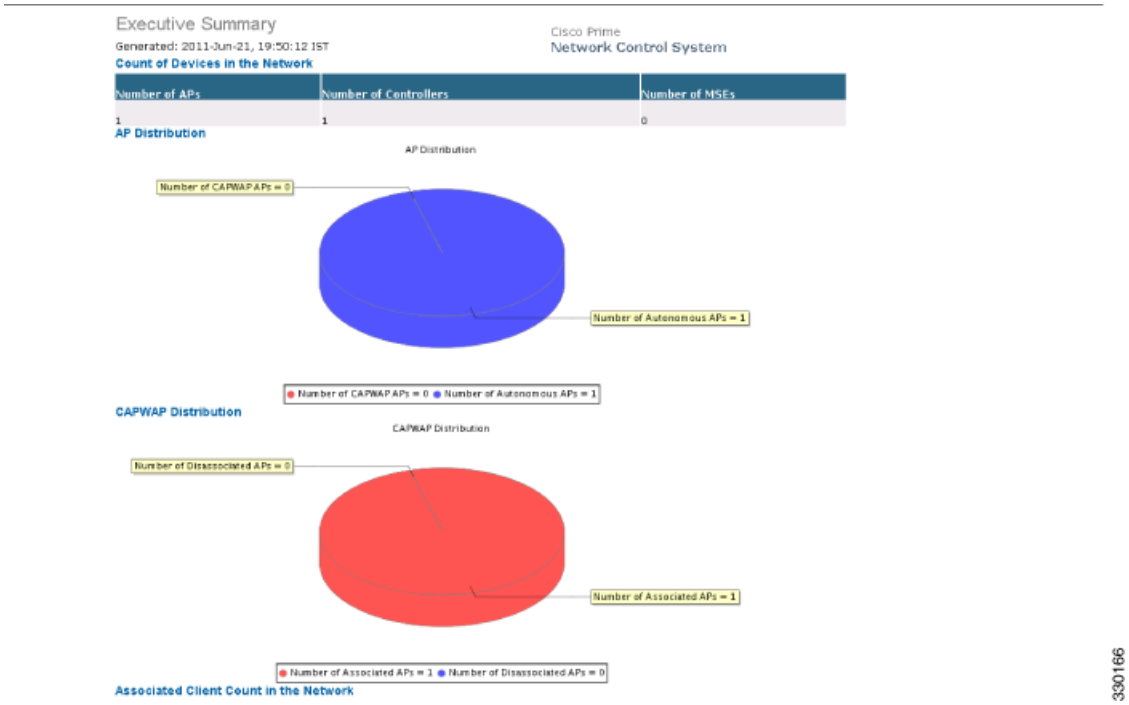
- Number of guest client in the network during the specified period of time (line graph).
- Throughput (Kbps) of clients by protocol during the specified period of time.
- Number of associated clients for each protocol during the specified period of time.
- Network utilization (%) during the specified period of time.
- Air Quality vs Time for each interface.
- Top 10 worst 5 GHz interferers in the network.
- Top 10 worst 2.4 GHz interferers in the network.

Note The Severity 1 refers to the best interferer and Severity 100 refers to the worst interferer in the top 10 worst 5 GHz and 2.4 GHz interferers in the network reports.

Note Executive Summary AP count includes disassociated AP(s) so if you have deleted a controller from NCS, the CAPWAP count in the report will also reflect the disassociated AP count.

Note The disassociated access points with model and serial number as **null** or **''** values will be filtered out from the Executive Summary reports.

Figure 14-40 Executive Summary Report Results



Performance Reports

Click **New** for a Performance Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

This section contains the following performance reports:

- 802.11 Counters
- Coverage Hole
- Network Utilization
- Traffic Stream Metrics
- Tx Power and Channel
- VoIP Calls Graph
- VoIP Calls Table
- Voice Statistics

802.11 Counters

This report displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

Click **802.11 Counters** from the Report Launch Pad to open the 802.11 Counters Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the 802.11 Counters Reports page. See the "Configuring an 802.11 Counters Report" section on page 14-144 and the "802.11 Counters Report Results" section on page 14-146 for more information.

Configuring an 802.11 Counters Report

This section describes how to configure an 802.11 Counters report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for 802.11 Counters report results contain the following:

- Time—The date and time of the count.
- AP Name—The name of the applicable access point.
- Slot—The slot number.
- Radio Type—802.11a/n or 802.11b/g/n.
- Tx Fragment Count—The number of successfully received MPDUs of type Data or Management.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- FCS Error Count—The number of FCS errors detected in a received MPDU.
- Retry Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multicast Rx Frame Count—The number of MSDUs received with the multicast bit set in the destination MAC address.
- Multicast Tx Frame Count—The number of times a multicast bit is set in the destination MAC address of a successfully transmitted MSDU. Operating as an STA in an ESS, where these frames are directed to the access point, implies having received an acknowledgment to all associated MPDUs.

- Tx Failed Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multiple Retry Count—The number of MSDUs successfully transmitted after more than one retransmission.
- Frame Duplicate Count—The number of times a frame is received that the Sequence Control field indicates is a duplicate.
- Tx Frame Count—The number of successfully transmitted MSDUs.
- RTS Success Count—The number of times a CTS is received in response to an RTS.
- RTS Failure Count—The number of times a CTS is not received in response to an RTS.
- ACK Failure Count—The number of times an ACK is not received when expected.
- WEP Undecryptable Count—The number of times a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the MAC address of the AT indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

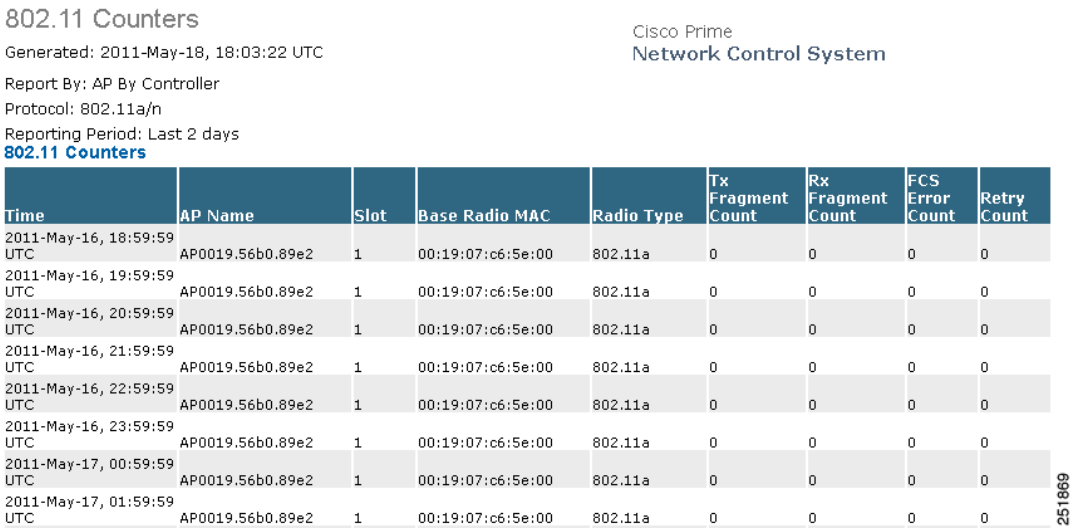
802.11 Counters Report Results

The following are potential results for an 802.11 Counters report, depending on how the report is customized (see Figure 14-41):

- Time (mandatory column)
- AP Name (mandatory column)
- Slot (mandatory column)
- AP MAC Address (mandatory column)
- Radio Type—802.11a/n or 802.11b/g/n.
- Tx Fragment Count—The number of successfully received MPDUs of type Data or Management.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- FCS Error Count—The number of FCS errors detected in a received MPDU.
- Retry Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multicast Rx Frame Count—The number of MSDUs received with the multicast bit set in the destination MAC address.
- Multicast Tx Frame Count—The number of time a multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this implies having received an acknowledgment to all associated MPDUs.
- Tx Failed Count—The number of unsuccessful MSDUs transmissions.
- Multiple Retry Count—The number of MSDUs successfully transmitted after more than one retransmission.
- Frame Duplicate Count—The number of times a frame is received that the Sequence Control field indicates is a duplicate.
- Tx Frame Count—The number of successfully transmitted MSDUs.
- RTS Success Count—The number of times a CTS is received in response to an RTS.

- RTS Failure Count—The number of times a CTS is not received in response to an RTS.
- ACK Failure Count—The number of times an ACK is not received when expected.
- WEP Undecryptable Count—The number of times a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the AT MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

Figure 14-41 802.11 Counters Report Results



802.11 Counters

Generated: 2011-May-18, 18:03:22 UTC

Cisco Prime
Network Control System

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 2 days

802.11 Counters

Time	AP Name	Slot	Base Radio MAC	Radio Type	Tx Fragment Count	Rx Fragment Count	FCS Error Count	Retry Count
2011-May-16, 18:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 19:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 20:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 21:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 22:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 23:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-17, 00:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-17, 01:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0

251869

Coverage Hole

This report identifies the location of potential coverage holes in your network and whether they occur more frequently at a given spot. This report can help you modify RRM settings or determine if additional access points are needed to provide coverage in sparsely deployed areas. It runs on the alarm table and shows both the alarm generation time, the cleared time (if cleared), and the state of the alarm (active or cleared).

Click **Coverage Hole** from the Report Launch Pad to open the Coverage Hole Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Coverage Hole Reports page. See the "Configuring a Coverage Hole Report" section on page 14-147 and the "Coverage Hole Report Results" section on page 14-149 for more information.

Configuring a Coverage Hole Report

This section describes how to configure a Coverage Hole report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.

- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Coverage Hole report results contain the following:

- Time—The date and time the coverage hole was detected.
- State—Clear or Active.
- AP Base Radio MAC Address—The MAC address of the access point base radio.
- AP Name—The name of the access point on which the coverage hole was detected.
- Radio Type—802.11a/n or 802.11b/g/n.
- Failed Clients.
- Total Clients.
- Threshold RSSI.
- Worst Client MAC.

- Worst Client RSSI.

Coverage Hole Report Results

The following are potential results for a Coverage Hole report, depending on how the report is customized (see Figure 14-42):

- Time (mandatory column)—Indicates the date and time that the alarm was generated or cleared (depending on the current state).
- State (mandatory column)—Active or cleared.
- AP Name (mandatory column)—The name of the access point on which the coverage hole was detected.
- Radio Type (mandatory column)—802.11a/n or 802.11b/g/n.
- AP Base Radio MAC Address.
- Failed Clients—The number of clients that have failed due to coverage hole issues.
- Total Clients—The number of total clients associated to this access point.
- Threshold RSSI—The lowest radio signal strength indication limit.
- Worst Client MAC—The MAC address of the client most affected by coverage hole issues.
- Worst Client RSSI—The radio signal strength indication of the client most affected by coverage hole issues.

Figure 14-42 Coverage Hole Report Results

Coverage Hole

Generated: 2011-May-18, 18:06:33 UTC

Report By: AP By Controller

Reporting Period: Last 1 day

Cisco Prime
Network Control System

Coverage Holes in the Network

notificationTimestamp	State	AP Name	Radio Type	Failed Clients	Total Clients	Worst Client RSSI
2011-May-18, 14:46:55 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:19:14 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-82
2011-May-17, 19:20:47 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:22:21 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-84
2011-May-17, 19:23:54 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:42:36 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-81
2011-May-17, 19:48:49 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:51:56 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-82
2011-May-17, 19:53:30 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0

Network Utilization

This report shows the overall network utilization based on the aggregated port utilization of all controllers on your network. These statistics can help identify current network performance and help with capacity planning for future scalability needs.

Note Average utilization (%) is the percentage of utilization where utilization is calculated as ((Tx+Rx)/Bandwidth).

Click **Network Utilization** from the Report Launch Pad to open the Network Utilization Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Network Utilization Reports page. See the "Configuring a Network Utilization Report" section on page 14-150 and the "Network Utilization Report Results" section on page 14-151 for more information.

Configuring a Network Utilization Report

This section describes how to configure a Network Utilization report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available data fields column.

Available information for the Network Utilization report results contain the following:

- Time
- Average Utilization (%)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.
- Average Tx (Mbps)—The average aggregated received Mbps of all ports on all controllers.
- Average Rx (Mbps)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.

Network Utilization Report Results

Network utilization is based on the average utilization of all the controllers in the network.

The following information is displayed for a Network Utilization report (see Figure 14-43):

- Time (mandatory column)
- Average Utilization (%) (mandatory column)—Average aggregated (totalDeltaBits/bandwidth) on all controllers.

Note Average utilization (%) is the percentage of utilization where utilization is calculated as ((Tx+Rx)/Bandwidth).

- Average Transmitting (in Mbps)—Average aggregated transmitted Megabytes of all ports on all controllers.
- Average Receiving (in Mbps)—Average aggregated received Megabytes of all ports on all controllers.

Figure 14-43 Network Utilization Report Results

Network Utilization

Generated: 2011-May-18, 18:08:30 UTC

Cisco Prime
Network Control System

Reporting Period: Last 2 days

Network Utilization

Network utilization is based on the average utilization of all the controllers in the network.

Time	Average Utilization (%)	Average Tx (Mbps)	Average Rx (Mbps)
2011-May-16, 18:59:59 UTC	0.09	0.48	0.45
2011-May-16, 19:59:59 UTC	0.10	0.45	0.48
2011-May-16, 20:59:59 UTC	0.10	0.49	0.59
2011-May-16, 21:59:59 UTC	0.11	0.50	0.51
2011-May-16, 22:59:59 UTC	0.08	0.44	0.47
2011-May-16, 23:59:59 UTC	0.12	0.58	0.66
2011-May-17, 00:59:59 UTC	0.09	0.44	0.49
2011-May-17, 01:59:59 UTC	0.08	0.44	0.41
2011-May-17, 02:59:59 UTC	0.08	0.44	0.43

251746

Traffic Stream Metrics

This report can be useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

Click **Traffic Stream Metrics** from the Report Launch Pad to open the Traffic Stream Metrics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Traffic Stream Metrics Reports page. See the "Configuring a Traffic Stream Metrics Report" section on page 14-152 and the "Traffic Stream Metrics Report Results" section on page 14-153 for more information.

Configuring a Traffic Stream Metrics Report

This section describes how to configure a Traffic Stream Metrics report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Traffic Stream Metrics report results contain the following:

- Time—Date and time the statistics were recorded.
- MAC address—The MAC address of the access point.
- AP Name—The access point name.

- Radio Type—802.11a/n or 802.11b/g/n.
- Average Queuing Delay (Downlink)—The average queuing delay for downlinks.
- Average Queuing Delay (Uplink)—The average queuing delay for uplinks.
- % Packet with less than 10 ms delay (downlink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for a downlink.
- % Packet with less than 10 ms delay (uplink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for an uplink.
- % Packet with more than 10 < 20 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for a downlink.
- % Packet with more than 10 < 20 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for an uplink.
- % Packet with more than 20 < 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for a downlink.
- % Packet with more than 20 < 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for an uplink.
- % Packet with more than 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for a downlink.
- % Packet with more than 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for an uplink.
- Packet Loss Ratio (Downlink)—The ratio of lost packets for downlinks.
- Packet Loss Ratio (Uplink)—The ratio of lost packets for uplinks.
- Total Packet Count (Downlink)—The total number of downlink packets.
- Total Packet Count (Uplink)—The total number of uplink packets.
- Roaming Count—Number of packets exchanged for roaming negotiations in this 90-second metrics page.
- Roaming Delay—Roaming delay in milliseconds.

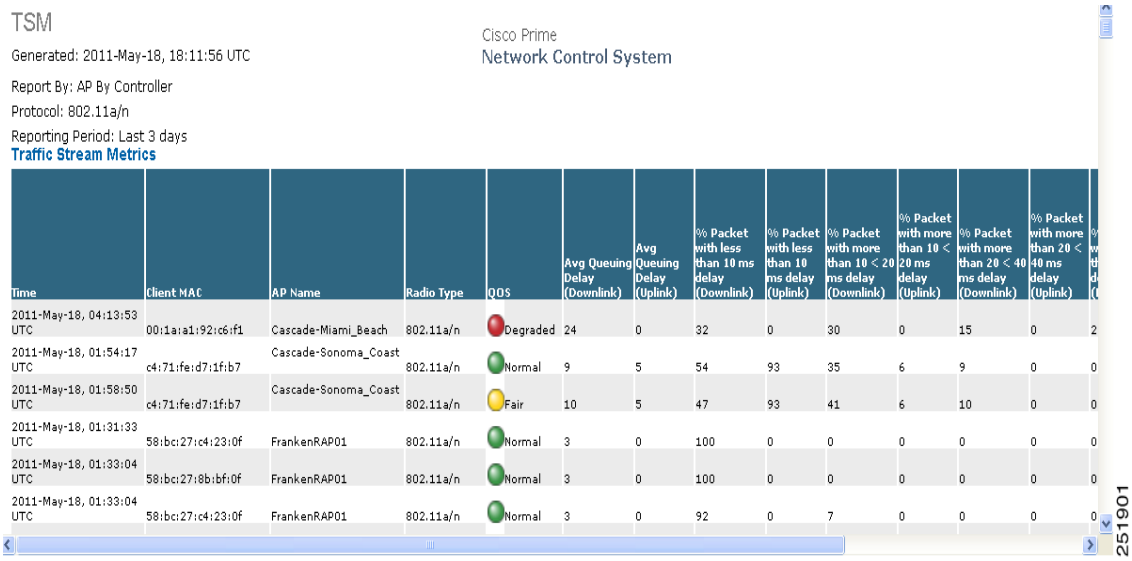
Traffic Stream Metrics Report Results

The following are potential results for a Traffic Stream Metrics report, depending on how the report is customized (see Figure 14-44):

- Time (mandatory column).
- MAC Address (mandatory column).
- AP Name (mandatory column).
- Radio Type (mandatory column).
- Average Queuing Delay (Downlink) (mandatory column).
- Average Queuing Delay (Uplink) (mandatory column).
- % Packet with less than 10 ms delay (downlink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for a downlink.
- % Packet with less than 10 ms delay (uplink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for an uplink.

- % Packet with more than 10 < 20 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for a downlink.
- % Packet with more than 10 < 20 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for an uplink.
- % Packet with more than 20 < 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for a downlink.
- % Packet with more than 20 < 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for an uplink.
- % Packet with more than 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for a downlink.
- % Packet with more than 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for an uplink.
- Packet Loss Ratio (Downlink)—The ratio of lost packets for downlinks.
- Packet Loss Ratio (Uplink)—The ratio of lost packets for uplinks.
- Total Packet Count (Downlink)—The total number of downlink packets.
- Total Packet Count (Uplink)—The total number of uplink packets.
- Roaming Count—Number of packets exchanged for roaming negotiations in this 90 seconds metrics page.
- Roaming Delay—Roaming delay in milliseconds.

Figure 14-44 Traffic Stream Metrics Report Results


TSM

Generated: 2011-May-18, 18:11:56 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

Cisco Prime
Network Control System

Traffic Stream Metrics

Time	Client MAC	AP Name	Radio Type	QOS	Avg Queuing Delay (Downlink)	Avg Queuing Delay (Uplink)	% Packet with less than 10 ms delay (Downlink)	% Packet with less than 10 ms delay (Uplink)	% Packet with more than 10 < 20 ms delay (Downlink)	% Packet with more than 10 < 20 ms delay (Uplink)	% Packet with more than 20 < 40 ms delay (Downlink)	% Packet with more than 20 < 40 ms delay (Uplink)	%
2011-May-18, 04:13:53 UTC	00:1a:a1:92:c6:f1	Cascade-Miami_Beach	802.11a/n	Degraded	24	0	32	0	30	0	15	0	2
2011-May-18, 01:54:17 UTC	c4:71:fe:d7:1f:b7	Cascade-Sonoma_Coast	802.11a/n	Normal	9	5	54	93	35	6	9	0	0
2011-May-18, 01:58:50 UTC	c4:71:fe:d7:1f:b7	Cascade-Sonoma_Coast	802.11a/n	Fair	10	5	47	93	41	6	10	0	0
2011-May-18, 01:31:33 UTC	58:bc:27:c4:23:0f	FrankenRAP01	802.11a/n	Normal	3	0	100	0	0	0	0	0	0
2011-May-18, 01:33:04 UTC	58:bc:27:8b:bf:0f	FrankenRAP01	802.11a/n	Normal	3	0	100	0	0	0	0	0	0
2011-May-18, 01:33:04 UTC	58:bc:27:c4:23:0f	FrankenRAP01	802.11a/n	Normal	3	0	92	0	7	0	0	0	0

251901

Tx Power and Channel

This report displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It helps to identify unexpected behavior or issues with network performance.

Click **Tx Power and Channel** from the Report Launch Pad to open the Tx Power and Channel Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Tx Power and Channel Reports page. See the "Configuring a Tx Power and Channel Report" section on page 14-155 and the "Tx Power and Channel Report Results" section on page 14-155 for more information.

Configuring a Tx Power and Channel Report

This section describes how to configure a Tx Power and Channel report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

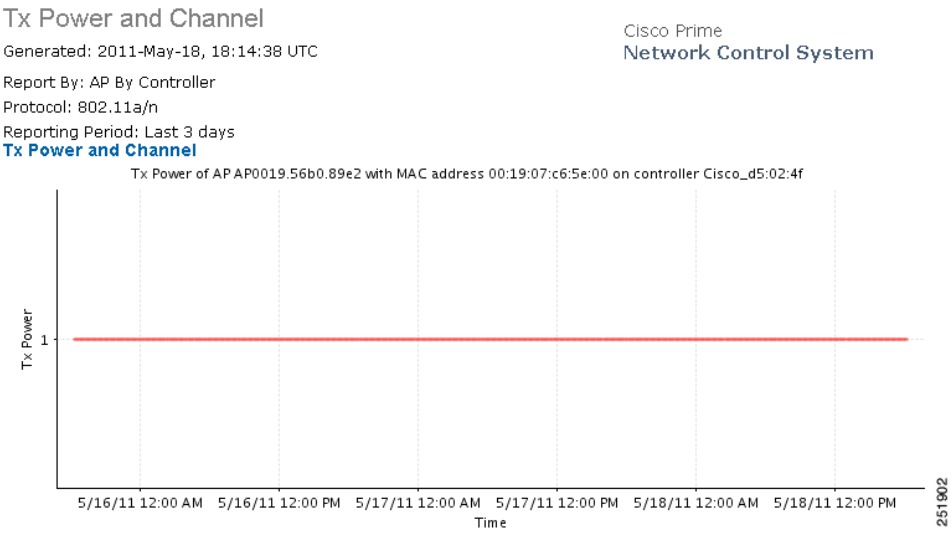
Tx Power and Channel Report Results

The following information is displayed for a Tx Power and Channel report (see Figure 14-45):

- Transmit power level for each access point during the specified period of time.

- Channel number for each access point during the specified period of time.

Figure 14-45 Tx Power and Channel Report Results



VoIP Calls Graph

This report helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click **VoIP Calls Graph** from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the VoIP Calls Graph Reports page. See the "Configuring a VoIP Calls Graph Report" section on page 14-156 and the "VoIP Calls Report Results" section on page 14-157 for more information.

Configuring a VoIP Calls Graph Report

This section describes how to configure a VoIP Calls Graph report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

- AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

VoIP Calls Report Results

The following information is displayed for a VoIP Calls Graph report:

- Number of attempted VoIP calls per radio during the specified period of time.
- Duration (in seconds) of VoIP calls.

VoIP Calls Table

This report helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a table.

Click **VoIP Calls Table** from the Report Launch Pad to open the VoIP Calls Table Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the VoIP Calls Table Reports page. See the "Configuring a VoIP Calls Table Report" section on page 14-157 and the "VoIP Calls Table Results" section on page 14-158 for more information.

Configuring a VoIP Calls Table Report

This section describes how to configure a VoIP Calls Table report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

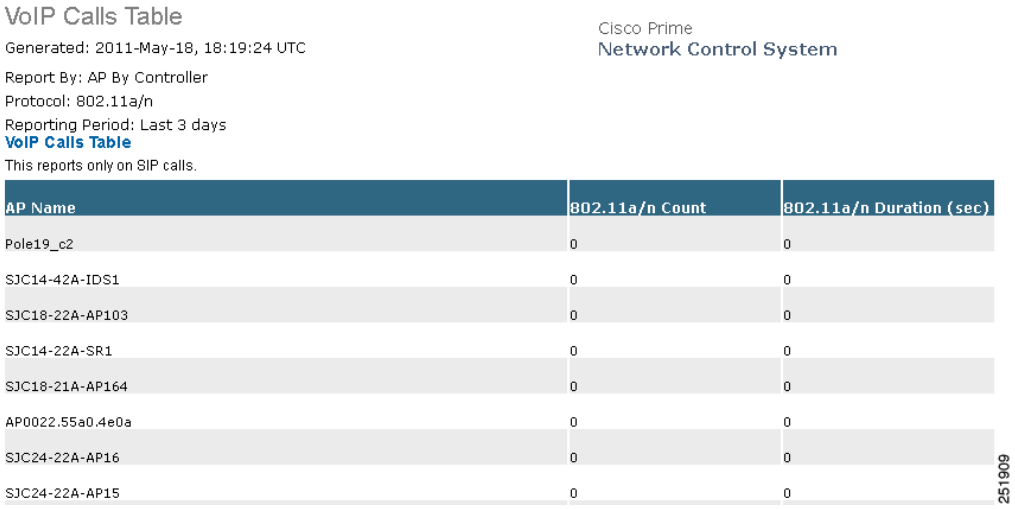
VoIP Calls Table Results

This report displays the same information as the VoIP Calls Graph report but the information is displayed in a table instead of a graph.

The following information is displayed for a VoIP Calls Table report (see Figure 14-46):

- Number of attempted VoIP calls per radio during the specified period of time.
- Duration (in seconds) of VoIP calls.

Figure 14-46 VoIP Calls Table Results



VoIP Calls Table

Generated: 2011-May-18, 18:19:24 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

VoIP Calls Table

This reports only on SIP calls.

Cisco Prime
Network Control System

AP Name	802.11a/n Count	802.11a/n Duration (sec)
Pole19_c2	0	0
SJC14-42A-IDS1	0	0
SJC18-22A-AP103	0	0
SJC14-22A-SR1	0	0
SJC18-21A-AP164	0	0
AP0022.55a0.4e0a	0	0
SJC24-22A-AP16	0	0
SJC24-22A-AP15	0	0

251909

Voice Statistics

This report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure Call Admission Control (CAC) is supported on voice clients.

Note Voice Statistics reports only apply to clients that support Call Admission Control (CAC) and have CAC enabled.

Click **Voice Statistics** from the Report Launch Pad to open the Voice Statistics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Voice Statistics Reports page. See the "Configuring a Voice Statistics Report" section on page 14-159 and the "Voice Statistics Results" section on page 14-160 for more information.

Configuring a Voice Statistics Report

This section describes how to configure a Voice Statistics report.

Settings

- Report Title—If you plan to used this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

- AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
- AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

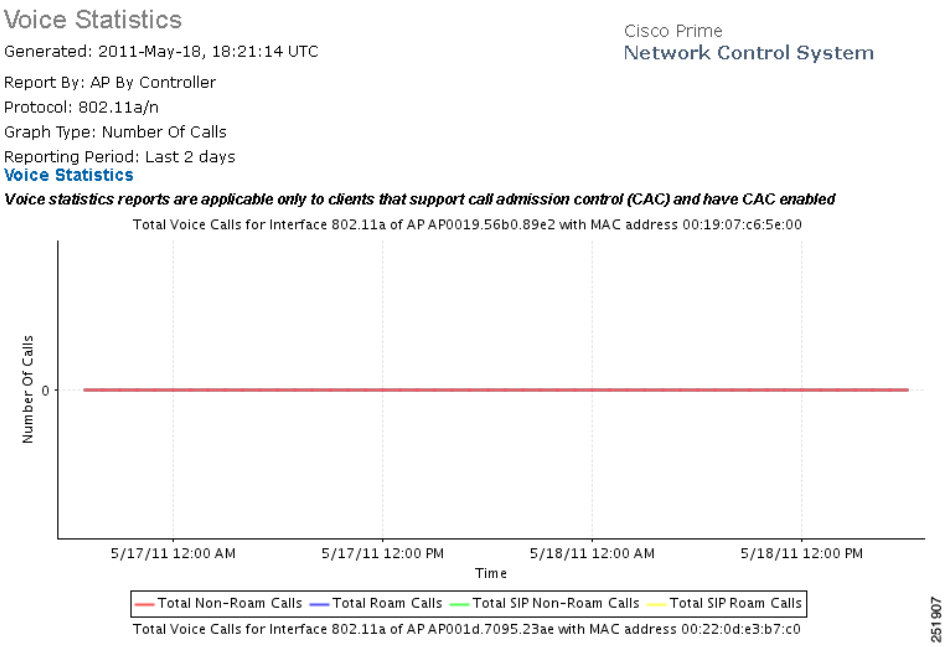
Voice Statistics Results

Note Voice Statistics reports only apply to clients that support Call Admission Control (CAC) and have CAC enabled.

The following information is displayed for a Voice Statistics report (see Figure 14-47):

- Percentage of bandwidth in use during the specified period of time.
- Total number of non-roaming and roaming calls during the specified period of time.
- Number of rejected calls during the specified period of time. Statistics include:
  - Total number of rejected calls.
  - Number of rejected roaming and non-roaming calls.
  - Number of rejected calls due to insufficient bandwidth, bad parameters, physical rate, and QoS policy.

Figure 14-47 Voice Statistics Results



Security Reports

Click **New** for a Security Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

This section contains the following Security Reports:

- Adaptive wIPS Alarm
- Adaptive wIPS Alarm Summary
- Adaptive wIPS Top 10 AP
- Adhoc Rogue Count Summary
- Adhoc Rogues
- New Rogue AP Count Summary
- New Rogue APs
- Rogue AP Count Summary
- Rogue APs
- Security Alarm Trending Summary

Adaptive wIPS Alarm

This report displays wIPS alarms by selected MSEs, controllers, and access points for each alarm type.

Click **Adaptive wIPS Alarms** from the Report Launch Pad to open the Adaptive wIPS Alarms Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adaptive wIPS Alarms Reports page. See the "Configuring an Adaptive wIPS Alarm Report" section on page 14-162 and the "Adaptive wIPS Alarm Report Results" section on page 14-163 for more information.

Configuring an Adaptive wIPS Alarm Report

This section describes how to configure an Adaptive wIPS Alarms report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE with Adaptive wIPS Service—Choose **All MSEs with Adaptive wIPS Service** from the Report Criteria drop-down list, or click **Edit** to choose a specific MSE.
  - Controller by MSE—Choose **All MSEs > All Controllers** from the Report Criteria drop-down list, or click **Edit** to choose a specific controller.
  - AP by MSE—Choose **All MSEs > All Controllers > All APs** from the Report Criteria drop-down list, or click **Edit** to choose a specific access point.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Alarm Category—Choose **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

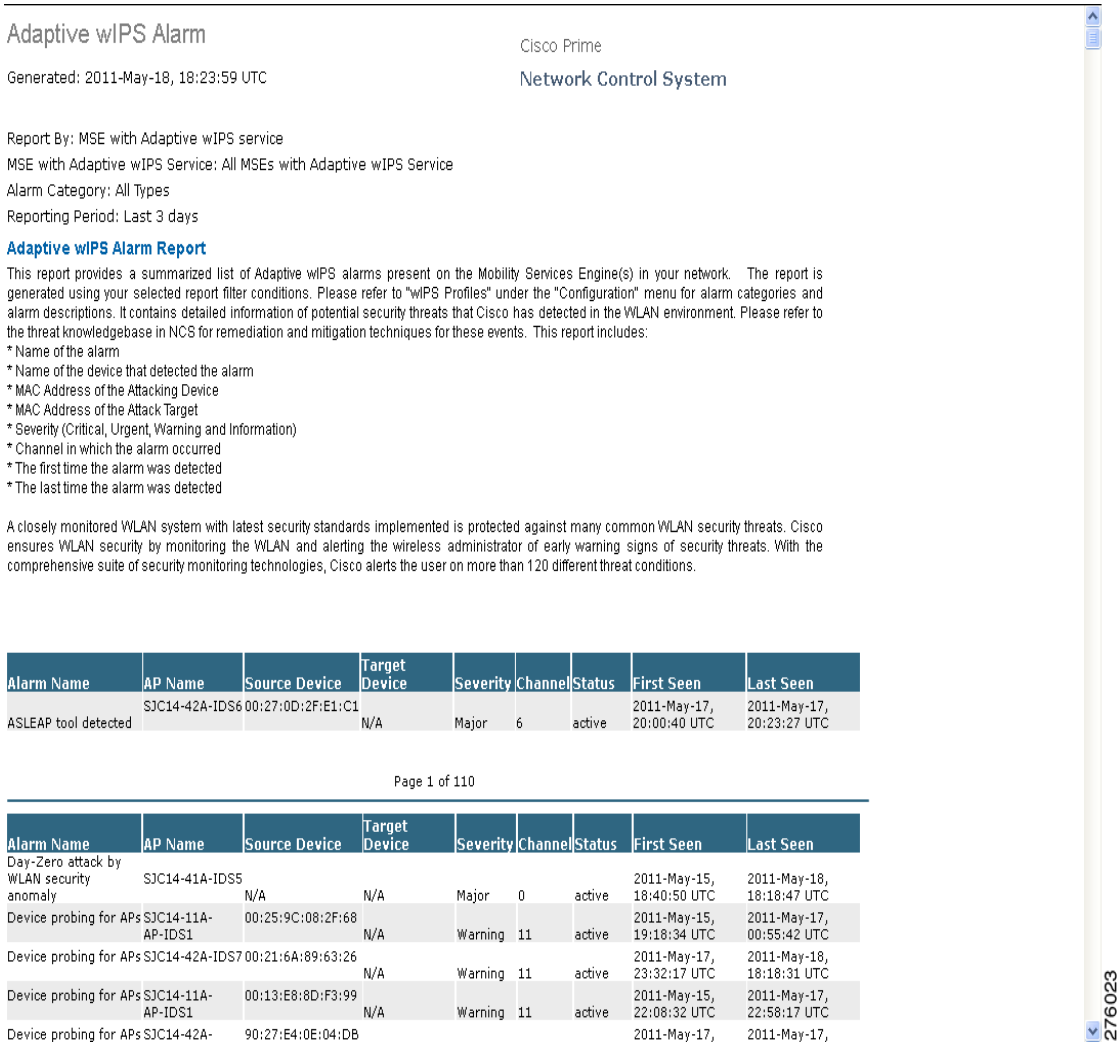
Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Adaptive wIPS Alarm Report Results

An Adaptive wIPS Alarm Report potentially contains the following information, depending on how the report is customized (see Figure 14-48):

- Alarm Name (mandatory column).
- AP Name—The name of the device that detected the alarm.
- Source Device—Identifies the device that initiated the potential attack.
- Target Device—Identifies the device targeted by the potential attack.
- Severity—Indicates the severity of the attack (Critical, Urgent, Warning, Information).
- Channel—The channel on which the alarm occurred.
- Status—The current status of the alarm (Active or Inactive).
- First Seen—The date and time the alarm was first detected.
- Last Seen—The date and time the alarm was last detected.
- AP MAC Address—The MAC address of this access point.
- Target SSID—The Service Set Identifier of the targeted device.
- Alarm Category.
- MSE Name—The name of the MSE to which this device is associated.

Figure 14-48 Adaptive wIPS Alarms Report



Adaptive wIPS Alarm

Cisco Prime
Network Control System

Generated: 2011-May-18, 18:23:59 UTC

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 3 days

Adaptive wIPS Alarm Report

This report provides a summarized list of Adaptive wIPS alarms present on the Mobility Services Engine(s) in your network. The report is generated using your selected report filter conditions. Please refer to "wIPS Profiles" under the "Configuration" menu for alarm categories and alarm descriptions. It contains detailed information of potential security threats that Cisco has detected in the WLAN environment. Please refer to the threat knowledgebase in NCS for remediation and mitigation techniques for these events. This report includes:
* Name of the alarm
* Name of the device that detected the alarm
* MAC Address of the Attacking Device
* MAC Address of the Attack Target
* Severity (Critical, Urgent, Warning and Information)
* Channel in which the alarm occurred
* The first time the alarm was detected
* The last time the alarm was detected

A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.

Alarm Name	AP Name	Source Device	Target Device	Severity	Channel	Status	First Seen	Last Seen
ASLEAP tool detected	SJC14-42A-IDS6	00:27:0D:2F:E1:C1	N/A	Major	6	active	2011-May-17, 20:00:40 UTC	2011-May-17, 20:23:27 UTC

Page 1 of 110

Alarm Name	AP Name	Source Device	Target Device	Severity	Channel	Status	First Seen	Last Seen
Day-Zero attack by WLAN security anomaly	SJC14-41A-IDS5	N/A	N/A	Major	0	active	2011-May-15, 18:40:50 UTC	2011-May-18, 18:18:47 UTC
Device probing for APs	SJC14-11A-AP-IDS1	00:25:9C:08:2F:68	N/A	Warning	11	active	2011-May-15, 19:18:34 UTC	2011-May-17, 00:55:42 UTC
Device probing for APs	SJC14-42A-IDS7	00:21:6A:89:63:26	N/A	Warning	11	active	2011-May-17, 23:32:17 UTC	2011-May-18, 18:18:31 UTC
Device probing for APs	SJC14-11A-AP-IDS1	00:13:E8:8D:F3:99	N/A	Warning	11	active	2011-May-15, 22:08:32 UTC	2011-May-17, 22:58:17 UTC
Device probing for APs	SJC14-42A-	90:27:E4:0E:04:DB					2011-May-17,	2011-May-17,

276023

Adaptive wIPS Alarm Summary

This report displays a summary of all the Adaptive wIPS Alarms on your network.

Click **Adaptive wIPS Alarm Summary** from the Report Launch Pad to open the Adaptive wIPS Alarm Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adaptive wIPS Alarm Summary Reports page. See the "Configuring an Adaptive wIPS Alarm Summary Report" section on page 14-164 and the "Adaptive wIPS Alarm Summary Report Results" section on page 14-165 for more information.

Configuring an Adaptive wIPS Alarm Summary Report

This section describes how to configure an Adaptive wIPS Alarm Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - MSE with Adaptive wIPS Service—Choose **All MSEs with Adaptive wIPS Service** from the Report Criteria drop-down list or click **Edit** to choose a specific MSE.
  - Controller by MSE—Choose **All MSEs > All Controllers** from the Report Criteria drop-down list or click **Edit** to choose a specific controller.
  - AP by MSE—Choose **All MSEs > All Controllers > All APs** from the Report Criteria drop-down list or click **Edit** to choose a specific access point.

Note In the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Alarm Category—Choose **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to be displayed in the results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

Adaptive wIPS Alarm Summary Report Results

An Adaptive wIPS Alarm Summary Report potentially contains the following information, depending on how the report is customized (see Figure 14-49):

- Alarm Name (mandatory column)

- Category—Alarm category
- Severity Information
  - Critical—The number of critical alarms for this access point.
  - Major—The number of major alarms for this access point.
  - Minor—The number of minor alarms for this access point.
  - Warning—The number of warning alarms for this access point.
- Total—The number of total alarms for this access point.

Figure 14-49 Adaptive wIPS Alarm Summary Report

Adaptive wIPS Alarm Summary

Generated: 2011-May-18, 18:28:19 UTC

Cisco Prime
Network Control System

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 3 days
Show: Up to 10 records

Page 1 of 3

Adaptive wIPS Alarm Summary Report

This report provides a consolidated list of all the alarms categories (Security IDS/IPS and Performance Intrusion) that have occurred in the WLAN environment. An insecure network can usually be fixed by reconfiguring some of the network equipment, by using additional software or hardware and always being in the forefront of implementing the latest security standards to provide good security for sensitive data such as employee salary data or company financial information. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. AirMagnet ensures WLAN performance and efficiency by monitoring the WLAN and alerting the wireless administrator on early warning signs for trouble. This includes reporting the devices which are vulnerable to violations/are violating and actions that can be performed to nullify such violations. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more 50 different threat conditions. The report includes the different types of policy violations categories, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning). Please refer to the Configure>wIPS Profiles to view all the possible alarm categories. threat knowledgebase in NCS for remediation and mitigation techniques for these events. A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.This report includes the different types of potential security threats, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning) for each of the Top 10 APs. Please refer to "wIPS Profiles" under the "Configuration" menu to view all detected alarms and their respective category.

AlarmName	Category	Critical	Major	Minor	Warning	Total
Unauthorized association by vendor list	wIPS - Security Penetration	26455	0	0	0	26455
Suspicious after-hours traffic detected	wIPS - Security Penetration	0	0	25555	0	25555
Spoofed MAC address detected	wIPS - Security Penetration	0	7829	0	0	7829
DoS: CTS flood	wIPS - Denial of Service Attack	6656	0	0	0	6656
DoS: RTS flood	wIPS - Denial of Service Attack	5451	0	0	0	5451
Unauthorized association detected	wIPS - Security Penetration	2711	0	0	0	2711
Malformed 802.11 packets detected	wIPS - Security Penetration	0	2024	0	0	2024

282613

Page 2 of 3

Adaptive wIPS Top 10 AP

This report displays the top ten access points with the highest number of generated Adaptive wIPS alarms.

Click **Adaptive wIPS Top 10 APs** from the Report Launch Pad to open the Adaptive wIPS Top 10 APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adaptive wIPS Top 10 APs Reports page. See the "Configuring an Adaptive wIPS Top 10 AP Report" section on page 14-167 and the "Adaptive wIPS Top 10 AP Report Results" section on page 14-168 for more information.

Configuring an Adaptive wIPS Top 10 AP Report

This section describes how to configure a wIPS Top 10 AP report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - MSE with Adaptive wIPS Service—Choose **All MSEs with Adaptive wIPS Service** from the Report Criteria drop-down list or click **Edit** to choose a specific MSE.
  - Controller by MSE—Choose **All MSEs > All Controllers** from the Report Criteria drop-down list or click **Edit** to choose a specific controller.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Alarm Category—Choose **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the results.

Note See the wIPS Policy Alarm Encyclopedia for more information regarding wIPS alarm types.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Adaptive wIPS Top 10 AP Report Results

An Adaptive wIPS Top 10 AP report potentially contains the following information, depending on how the report is customized (see Figure 14-50):

- AP Name (mandatory column)
- Critical—The number of critical alarms for this access point.
- Major—The number of major alarms for this access point.
- Minor—The number of minor alarms for this access point.
- Warning—The number of warning alarms for this access point.
- Total—The number of total alarms for this access point.
- AP MAC Address—The MAC address of this access point.
- MSE Name—The name of the MSE to which this access point is associated.

Figure 14-50 Adaptive wIPS Top 10 APs Report

Adaptive wIPS Top 10 AP

Generated: 2011-May-18, 18:41:33 UTC

Cisco Prime
Network Control System

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 3 days

Adaptive wIPS Top 10 AP Report

This report provides a list of the top 10 wIPS monitoring APs that have detected the most security alarms that have occurred in the WLAN environment. These alarms are stored on the Mobility Services Engine(s) installed on your network running Adaptive wIPS. A high number of alarms on a monitoring AP is indicative of "security hot spots" in the network that warrant closer investigation. Please refer to the threat knowledgebase in WCS for remediation and mitigation techniques for these events. A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.This report includes the different types of potential security threats, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning) for each of the Top 10 APs. Please refer to "wIPS Profiles" under the "Configuration" menu to view all detected alarms and their respective category.

AP Name	Critical	Major	Minor	Warning	Total
SJC14-11A-AP-IDS1	270	5	36	11	322

Page 1 of 2

275947

Adhoc Rogue Count Summary

This report displays a summarized count of all adhoc rogue access points.

Click **Adhoc Rogue Count Summary** from the Report Launch Pad to open the Adhoc Rogue Count Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adhoc Rogue Count Summary Reports page. See the "Configuring an Adhoc Rogue Count Summary Report" section on page 14-169 and the "Adhoc Rogue Count Summary Report Results" section on page 14-170 for more information.

Configuring an Adhoc Rogue Count Summary Report

This section describes how to configure an Adhoc Rogue Count Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

Note In the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to be displayed in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

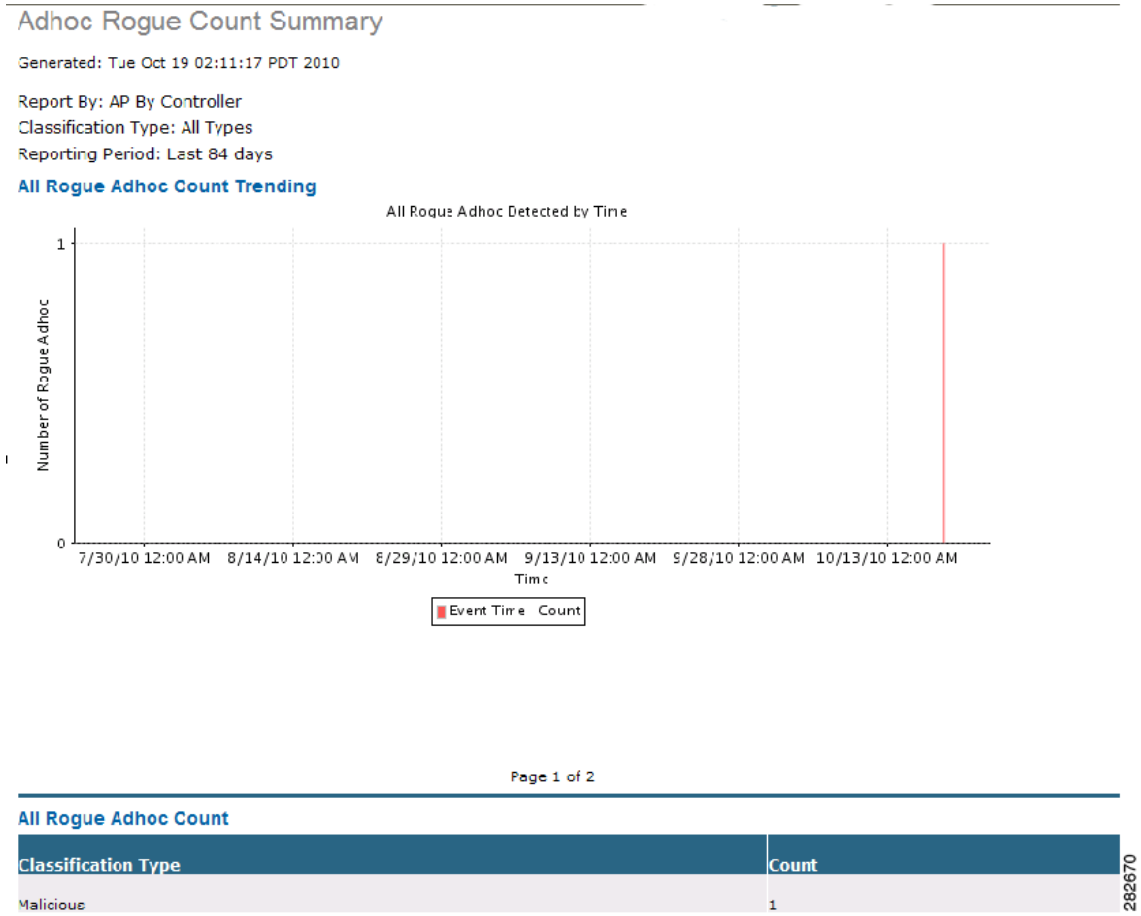
Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

Adhoc Rogue Count Summary Report Results

The following are potential results for an Adhoc Rogue Count Summary report, depending on how the report is customized (see Figure 14-51):

Figure 14-51 Adhoc Rogue Count Summary Report



Adhoc Rogue Events

This report displays all adhoc rogue events received by NCS.

The following settings and scheduling parameters are available for this report:

Click **Adhoc Rogue Events** from the Report Launch Pad to open the Adhoc Rogue Events Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adhoc Rogue Events Reports page. See the "Configuring an Adhoc Rogue Events Report" section on page 14-171 and the "Adhoc Rogue Events Report Results" section on page 14-172 for more information.

Configuring an Adhoc Rogue Events Report

Settings

The following settings can be configured for an Adhoc Rogue Events report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note From the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period

Note Reporting period is based on the alarm Last Seen time.

  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" for more information on customizing report results.

Note Mandatory columns are displayed in blue font and cannot be moved to Available Columns. Last Seen Time, Rogue MAC Address, and Detecting AP Name are mandatory columns for the Adhoc Rogue Events report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Adhoc Rogue Events Report Results

The following are potential results for an Adhoc Rogue Events report, depending on how the report is customized:

- Last Seen Time (mandatory column)
- Rogue MAC Address (mandatory column)
- Detecting AP Name (mandatory column)
- Radio Type—802.11a or 802.11b/g.
- Controller IP Address—The IP address of the controller on which the adhoc rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the adhoc rogue was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Adhoc rogue radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the adhoc rogue.
- RSSI (dBm)—The received signal strength indicator in dBm.

Adhoc Rogues

This report displays details for all adhoc rogue devices detected by your network access points based on the time they were last seen.

NCS receives updates about adhoc rogues from controllers by using traps or by polling. Last Seen Time is updated anytime a trap for the adhoc rogue is received or the adhoc rogue was seen during the last polling cycle of NCS.

Note This report includes rogue access point alarms with clear severity.

Click **Adhoc Rogues** from the Report Launch Pad to open the Adhoc Rogues Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adhoc Rogues Reports page. See the "Configuring an Adhoc Rogues Report" section on page 14-173 and the "Adhoc Rogues Report Results" section on page 14-174 for more information.

Configuring an Adhoc Rogues Report

This section describes how to configure an Adhoc Rogues report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Adhoc Rogues Report Results

The following are potential results for an Adhoc Rogues report, depending on how the report is customized (see Figure 14-52):

- Last Seen Time—Date and time the ad hoc rogue was last seen.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller that supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the ad hoc rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Ad hoc rogue radios appear as “Alert” when first scanned by the port, or as “Pending” when operating system identification is still underway.
- Rogue MAC Address—The MAC address of the ad hoc rogue.
- Channel Number—The channel number of the ad hoc rogue.
- RSSI (dBm)—The maximum received signal strength indicator ever reported by any controller for this rogue.

Figure 14-52 Adhoc Rogues Results

Adhoc Rogues

Generated: 2011-May-18, 18:50:02 UTC

Report By: AP By Controller

Reporting Period: Last 2 days

Cisco Prime
Network Control System

Adhoc Rogues

Last Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Severity
2011-May-18, 11:00:43 UTC	1a:9a:dd:87:d1:39	SJC24-31A-AP27	802.11b/g/n	10.32.34.2	System Campus > SJC-24 > 3rd Floor	Brent Mower's Guest Network	Removed	Clear
2011-May-18, 17:16:00 UTC	08:61:08:00:45:00	SJC14-41A-IDS8	802.11b/g/n	10.32.34.2			Alert	Minor
2011-May-18, 17:15:35 UTC	09:47:08:00:45:00	SJC14-41A-ROBERT-MOSES	802.11b/g/n	10.32.34.2			Alert	Minor
2011-May-18, 17:16:08 UTC	06:25:84:09:1e:ee	SJC19-42A-AP207	802.11b/g/n	10.32.34.2	System Campus > SJC-19 > 4th Floor	bb-voice	Alert	Minor
2011-May-18, 17:16:17 UTC	06:25:84:09:23:2a	SJC19-42A-AP207	802.11b/g/n	10.32.34.2	System Campus > SJC-19 > 4th Floor	cisco-32-voice	Alert	Minor
2011-May-18, 17:16:17 UTC	06:25:84:09:22:ce	SJC19-42A-AP207	802.11b/g/n	10.32.34.2	System Campus > SJC-19 > 4th Floor	uc320-voice-acwang	Alert	Minor
2011-May-17, 20:14:49 UTC	8a:43:e1:ab:00:d5	SJC19-42A-AP207	802.11b/g/n	10.32.37.6	System Campus > SJC-19 > 4th Floor	asterisk	Alert	Minor
2011-May-17, 03:28:12 UTC	00:26:4a:da:03:e0	SJC17-31A-P192	802.11b/g	10.34.142.150	System Campus > SJC-17 > 3rd Floor	hpsetup	Removed	Clear
2011-May-18, 17:17:48 UTC	00:16:35:9f:74:d2	SJC17-31A-P197	802.11b/g	10.34.142.150	System Campus > SJC-17 > 3rd Floor	hpsetup	Removed	Clear

251874

New Rogue AP Count Summary

This report displays a summarized count of all the new rogue access points.

Click **New Rogue AP Count Summary** from the Report Launch Pad to open the New Rogue AP Count Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the New Rogue AP Count Summary Reports page. See the "Configuring a New Rogue AP Count Summary Report" section on page 14-175 and the "New Rogue AP Count Summary Report Results" section on page 14-176 for more information.

Configuring a New Rogue AP Count Summary Report

This section describes how to configure a New Rogue AP Count Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to be displayed in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

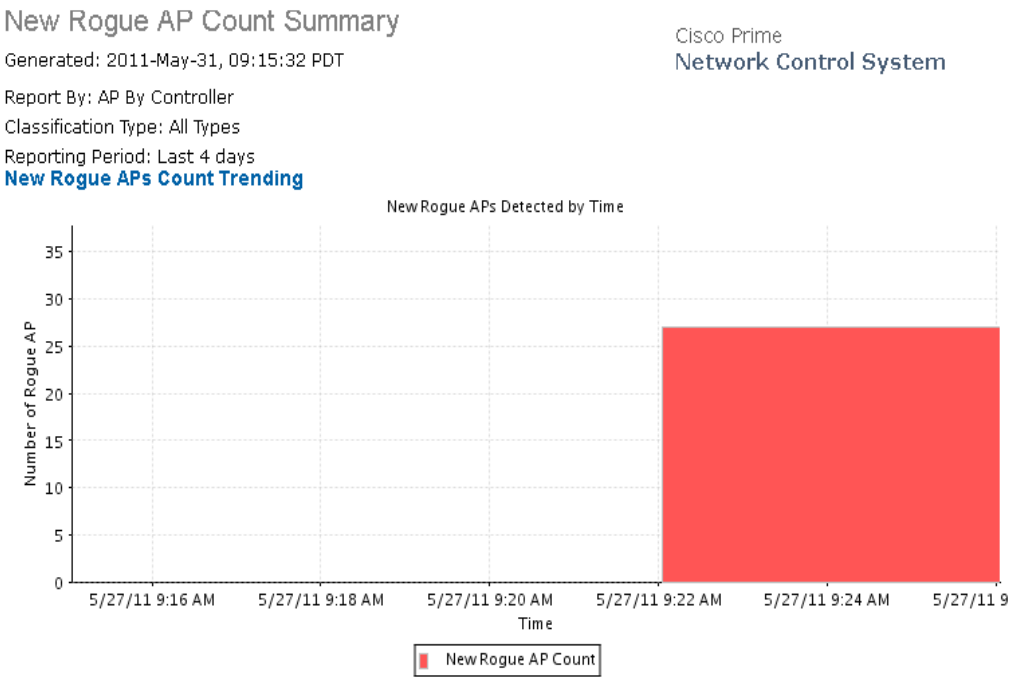
Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

New Rogue AP Count Summary Report Results

The following are potential results for a New Rogue AP Count Summary report, depending on how the report is customized (see Figure 14-53):

Figure 14-53 New Rogue AP Count Summary Report



New Rogue APs

This report displays all the new rogues detected for the first time on your network within the selected timeframe for this report. The value in the Created Time column indicates the time at which the rogue was first detected.

Note This report includes rogue access point alarms with clear severity.

Click **New Rogue AP** from the Report Launch Pad to open the New Rogue APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the New Rogue APs Reports page. See the "Configuring a New Rogue AP Report" section on page 14-176 and the "New Rogue AP Report Results" section on page 14-177 for more information.

Configuring a New Rogue AP Report

This section describes how to configure a New Rogue Access Points report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click Customize to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

New Rogue AP Report Results

The following are potential results for a New Rogue APs report, depending on how the report is customized (see Figure 14-54):

Note The results for this report are sorted based on First Time Seen.

- First Seen Time—The date and time the rogue access point was first seen.
- Rogue MAC Address—The MAC address of the rogue access point. Click the MAC address link to view the alarm details of the access point.

- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller that supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the rogue access point is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Rogue access point radios appear as “Alert” when first scanned by the port, or as “Pending” when operating system identification is still underway.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The received signal strength indicator in dBm.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).
- Switch Port Trace Status—Indicates whether or not the switch port was traced.
- Switch Port Trace Summary—Provides a summary of the switch port trace or remains blank if no switch port was traced.

Figure 14-54 New Rogue Access Points Report

New Rogue APs

Generated: 2011-May-18, 18:57:00 UTC

Report By: AP By Controller

On Network: All Types

Reporting Period: Last 3 days

Cisco Prime
Network Control System

New Rogue APs

First Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Classification Type	On Network
2011-May-18, 17:15:26 UTC	00:0f:f8:58:52:62	SJC24-11A-AP11	802.11b/g/n	10.32.34.2	System Campus > SJC-24 > 1st Floor	mobilevpn	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	00:21:d8:7e:73:74	wnbu-bgl11-41a-iap-ap3	802.11b/g	10.65.23.39			Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	00:1f:f3:02:da:cd	supusu-homeap	802.11b/g	171.70.35.135		2WIRE268	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	00:21:29:bf:6b:74	supusu-homeap	802.11b/g	171.70.35.135		Simba	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	08:17:35:c7:2c:8d	dwill-homeap	802.11a	171.70.35.135		Cisco-.1x	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	08:17:35:c7:2c:8c	dwill-homeap	802.11a	171.70.35.135		Cisco-open	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	08:17:35:c7:02:4d	dwill-homeap	802.11a	171.70.35.135		Cisco-.1x	Alert	Unclassified	No

251891

Rogue AP Count Summary

This report displays a summarized count of all the rogue access points on your network.

Click **Rogue AP Count Summary** from the Report Launch Pad to open the Rogue AP Count Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the “Managing Current Reports” section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Rogue AP Count Summary Reports page. See the "Configuring a Rogue AP Count Summary Report" section on page 14-179 and the "Rogue AP Count Summary Report Results" section on page 14-180 for more information.

Configuring a Rogue AP Count Summary Report

This section describes how to configure a Rogue AP Count Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to be displayed in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click Customize to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

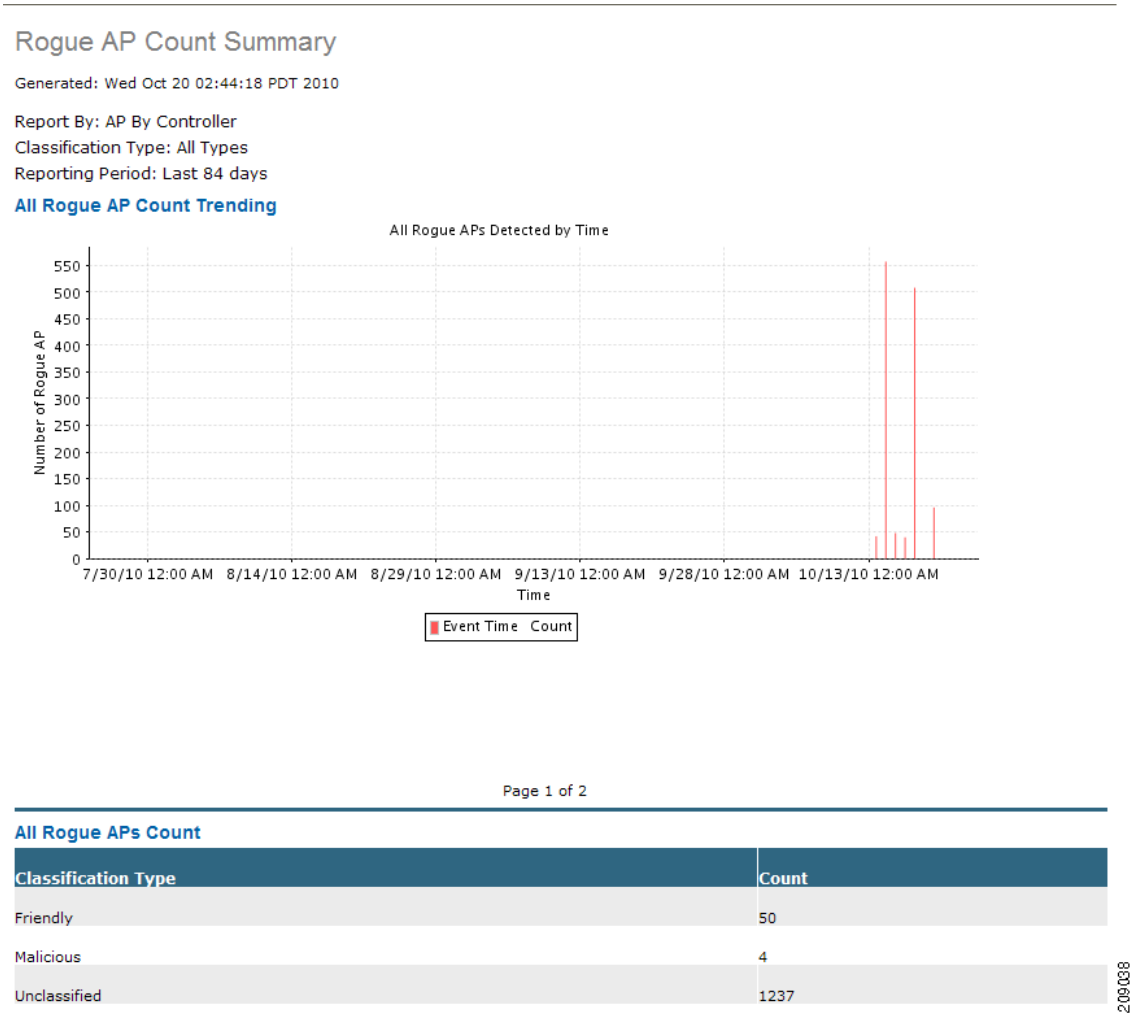
Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

Rogue AP Count Summary Report Results

The following are potential results for a New Rogue AP Count Summary report, depending on how the report is customized (see Figure 14-55):

- All Rogue AP Count Trending graph
- All Rogue AP Count based on classification type

Figure 14-55 Rogue AP Count Summary Report



Rogue Access Point Events

This report displays all rogue access point events received by NCS and based on the event time.

Any rogue-related trap received by NCS is logged as a rogue event in NCS. A new rogue access point event is created by NCS based on polled data when there is a newly detected rogue access point. In addition, an event is also created by NCS when the user changes the state and classification of the rogue access point through the NCS user interface.

Note One rogue can have multiple events. This report is based on the timestamp of the event.

Click **Rogue AP Events** from the Report Launch Pad to open the Rogue AP Events Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Rogue AP Events Reports page. See the "Configuring a Rogue Access Point Events Report" section on page 14-181 and the "Rogue AP Events Report Results" section on page 14-182 for more information.

Configuring a Rogue Access Point Events Report

Settings

The following settings can be configured for a Rogue Access Point Events report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

  Note From the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Mandatory columns are displayed in blue font and cannot be moved to Available Columns. Last Seen Time, Rogue MAC Address, and Detecting AP Name are mandatory columns for the Rogue Access Point Events report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Rogue AP Events Report Results

The following are potential results for a Rogue AP Events report, depending on how the report is customized:

- Last Seen Time (mandatory column)
- Rogue MAC Address (mandatory column)
- Detecting AP Name (mandatory column)
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point was detected.
- SSID—The user-defined Service Set Identifier name.

- State—The radio state relative to the network or port. Rogue access point radios appear as “Alert” when first scanned by the port, or as “Pending” when operating system identification is still underway.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The received signal strength indicator in dBm.
- SNR—The Signal-to-Noise Ratio.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).

Rogue APs

NCS gets updates about rogues from controllers by using traps or by polling. The Last Seen Time is updated anytime a trap for the rogue is received or rogue was seen during the last polling cycles of NCS.

This report displays all rogues detected by the access points in your network based on the “last seen time” of the rogue access points and the selected filtering criteria. It orders rogue access points based on the time they were last heard.

Note The report includes rogue access point alarms with clear severity.

Click **Rogue APs** from the Report Launch Pad to open the Rogue APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the “Managing Current Reports” section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Rogue APs Reports page. See the “Configuring a Rogue APs Report” section on page 14-183 and the “Rogue APs Report Results” section on page 14-184 for more information.

Configuring a Rogue APs Report

This section describes how to configure a Rogue APs report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Rogue APs Report Results

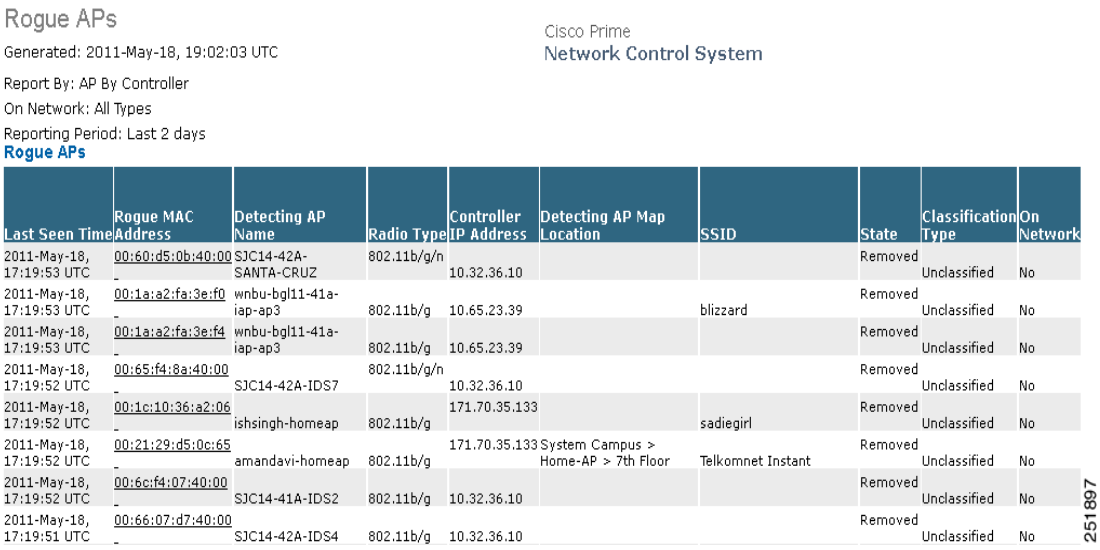
The following are potential results for a Rogue APs report, depending on how the report is customized (see Figure 14-56):

Note The results for this report are sorted by "Last Seen" time.

- Last Seen Time—The date and time the rogue access point was last detected.
- Rogue MAC Address—The MAC address of the rogue access point. Click an item under MAC Address to view Rogue AP details.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller which supports maximum RSSI.
- Radio Type—802.11a or 802.11b/g.
- Controller IP Address—The IP address of the controller on which the rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point is located.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Rogue access point radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The maximum received signal strength indicator ever reported by any controller for this rogue.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).

- Switch Port Trace Status—Indicates whether or not the switch port was traced.
- Switch Port Trace Summary—Provides a summary of the switch port trace or remains blank if no switch port was traced.
- On Network—Indicates whether the access point is on the network or not.

Figure 14-56 Rogues APs Report



Rogue APs

Generated: 2011-May-18, 19:02:03 UTC

Cisco Prime
Network Control System

Report By: AP By Controller

On Network: All Types

Reporting Period: Last 2 days

Rogue APs

Last Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Classification Type	On Network
2011-May-18, 17:19:53 UTC	00:60:d5:0b:40:00	SJC14-42A-SANTA-CRUZ	802.11b/g/n	10.32.36.10			Removed	Unclassified	No
2011-May-18, 17:19:53 UTC	00:1a:a2:fa:3e:f0	wnbu-bgl11-41a-iap-ap3	802.11b/g	10.65.23.39		blizzard	Removed	Unclassified	No
2011-May-18, 17:19:53 UTC	00:1a:a2:fa:3e:f4	wnbu-bgl11-41a-iap-ap3	802.11b/g	10.65.23.39			Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:65:f4:8a:40:00	SJC14-42A-IDS7	802.11b/g/n	10.32.36.10			Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:1c:10:36:a2:06	ishsingh-homeap	802.11b/g	171.70.35.133		sadiegirl	Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:21:29:d5:0c:65	amandavi-homeap	802.11b/g	171.70.35.133	System Campus > Home-AP > 7th Floor	Telkomnet Instant	Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:6c:f4:07:40:00	SJC14-41A-IDS2	802.11b/g	10.32.36.10			Removed	Unclassified	No
2011-May-18, 17:19:51 UTC	00:66:07:d7:40:00	SJC14-42A-IDS4	802.11b/g	10.32.36.10			Removed	Unclassified	No

251897

Security Alarm Trending Summary

This report displays a summary of trends of security alarms over a period of time.

Click **Security Alarm Trending Summary** from the Report Launch Pad to open the Security Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-13 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Security Summary Reports page. See the "Configuring a Security Alarm Trending Summary Report" section on page 14-185 and the "Security Alarm Trending Summary Report Results" section on page 14-186 for more information.

Configuring a Security Alarm Trending Summary Report

This section describes how to configure a Security Alarm Trending Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Security Alarm Trending Summary Report Results

The following are potential results for a Security Alarm Trending Summary report, depending on how the report is customized (see Figure 14-57):

Figure 14-57 Security Alarm Trending Summary Report