CHAPTER 17

Running Reports

Cisco WCS 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 WCS 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 from the last polling cycle without continuously polling
- Historical, which retrieves data from the device periodically and stores it in the WCS 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 WCS, 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 The number of rows visible in a report depends on the size of the html file, the number of database records, the size of the exported page, the size of the scheduled report, and the WCS server memory size. If you want the report to print as it appears on the page display, you must choose landscape mode. The detailed limitations are as follows:

Maximum number of graphs for a single report—500
Maximum size of an HTTP report (displayed in the Results parameter)—65 Mbs
Maximum number of records for a non-scheduled report—100,000 records
Maximum number of records for a scheduled report—Up to 200,000 records (when physical memory is greater than 1 GB)

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

- Report Launch Pad—The hub for all WCS reports. From this page, you can access specific types of reports and create new reports. See the "Report Launch Pad" section on page 17-2 for more information.
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in WCS. See the "Managing Scheduled Run Results" section on page 17-9 for more information.

- Saved Reports—Allows you to access and manage all currently saved reports in WCS. See the "Managing Saved Reports" section on page 17-11 for more information.

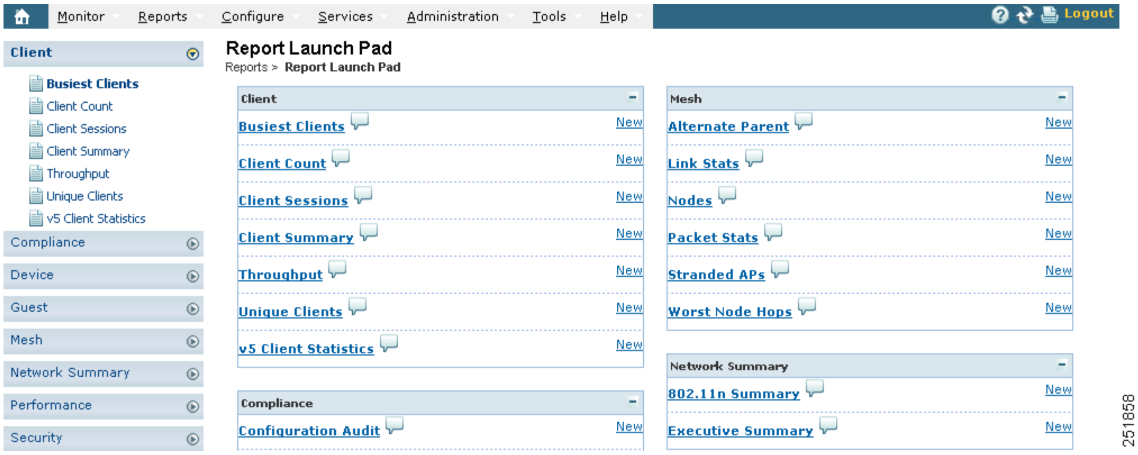
Note See the "Specific WCS Reports" section on page 17-13 for additional information for each report type.

Report Launch Pad

The report launch pad provides access to all WCS 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 17-1).

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

Figure 17-1 Report Launch Pad



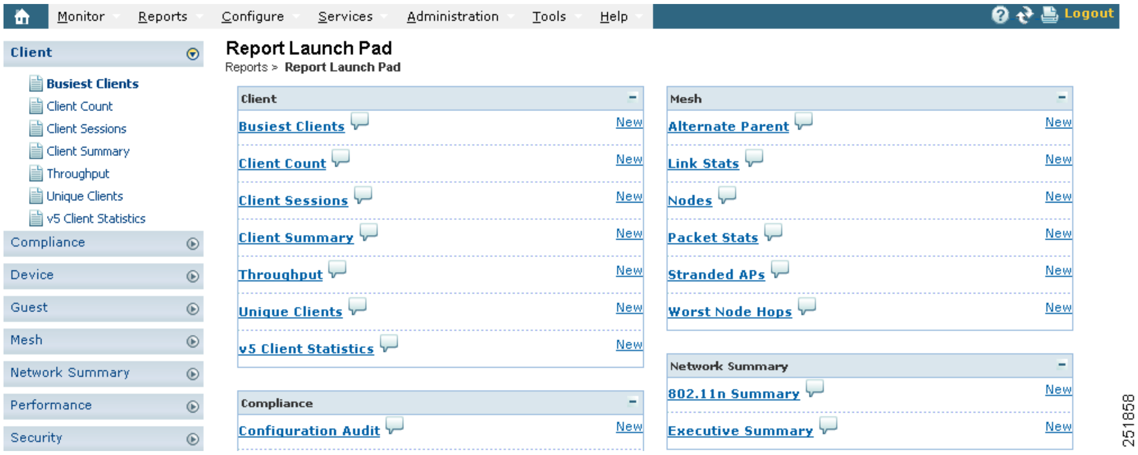
Creating and Running a New Report

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 17-2).

Figure 17-2 Report Launch Pad

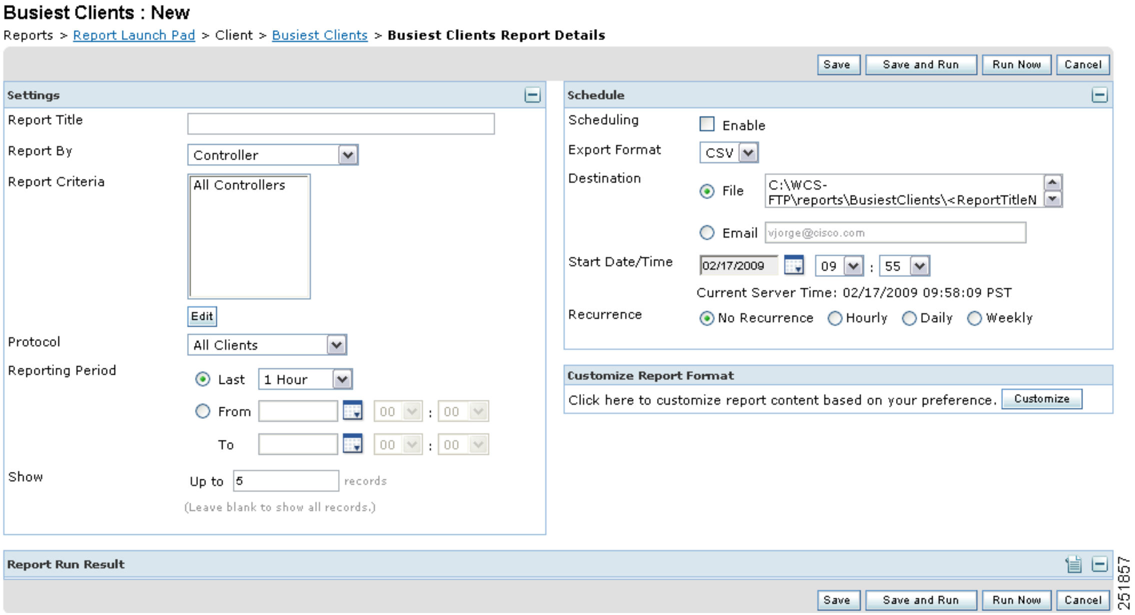


Step 2 Find the appropriate report in the main section of the Report Launch Pad.

> **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 reports for that report type.

Step 3 Click **New** to the right of the report. The Report Details page appears (see Figure 17-3).

Figure 17-3 Report Details Page



Busiest Clients : New

Reports > Report Launch Pad > Client > Busiest Clients > **Busiest Clients Report Details**

Settings

Report Title:
Report By: Controller
Report Criteria: All Controllers
Protocol: All Clients
Reporting Period: ● Last 1 Hour
○ From 00 : 00
To 00 : 00
Show: Up to 5 records
(Leave blank to show all records.)

Schedule

Scheduling: □ Enable
Export Format: CSV
Destination: ● File C:\WCS-FTP\reports\BusiestClients\<ReportTitleN
○ Email vjorge@cisco.com
Start Date/Time: 02/17/2009 09 : 55
Current Server Time: 02/17/2009 09:58:09 PST
Recurrence: ● No Recurrence ○ Hourly ○ Daily ○ Weekly

Customize Report Format

Click here to customize report content based on your preference.

Report Run Result

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, enter a report name.
- Report By—Select the appropriate Report By category from the drop-down list.
- 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.

- Protocol—Select 802.11a/n, 802.11b/g/n, or both.
- Report Period
  - Last—Select the **Last** radio button and 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. Select the hours and minutes from the drop-down lists.

Note The supported number of records for a report query is 1,00,000. If a report query retrieves more than 1,00,000 records, an error message is displayed to generate the report for a short reporting period so that the query retrieves less than 1,00,000 records.

- Show—Enter the number of records that you want displayed on each page.

Note 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—Select your destination type (File or Email). Enter the applicable file location or the email address.

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

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

Note To set the mail server setup for emails, choose **Administration > Settings**, then click **Mail Server** in the sidebar 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. Select the time from the hours and minutes drop-down lists. The report will begin running on this data and at this time.
- 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 17-1 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 17-1 Report Customization

Report	Customizable	Multiple Sub-Reports?	Report Views	Report View Customizable?
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	Yes	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic Stream Metrics	Yes	No	Tabular[1]	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	Yes	No	Tabular	No
AP Profile Status	Yes	No	Tabular	No
Device Summary	Yes	No	Tabular	No
Busiest APs	Yes	No	Tabular	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

Table 17-1 Report Customization

Report	Customizable	Multiple Sub-Reports?	Report Views	Report View Customizable?
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
WCS Guest Operations	Yes	No	Tabular	No
Alternate Parent	Yes	No	Tabular	No
Link Stats - Link Stats	Yes	No	Tabular	No
Link Stats - Node Hops	Yes	No	Graphical	No
Nodes	Yes	No	Tabular	No
Packet Stats - Packet Stats	No	No	Graphical	No
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 Top 10 APs	Yes	No	Tabular	No
Adhoc Rogue Events	Yes	No	Tabular	No
Adhoc Rogues	Yes	No	Tabular	No
New Rogue APs	Yes	No	Tabular	No

Table 17-1 Report Customization

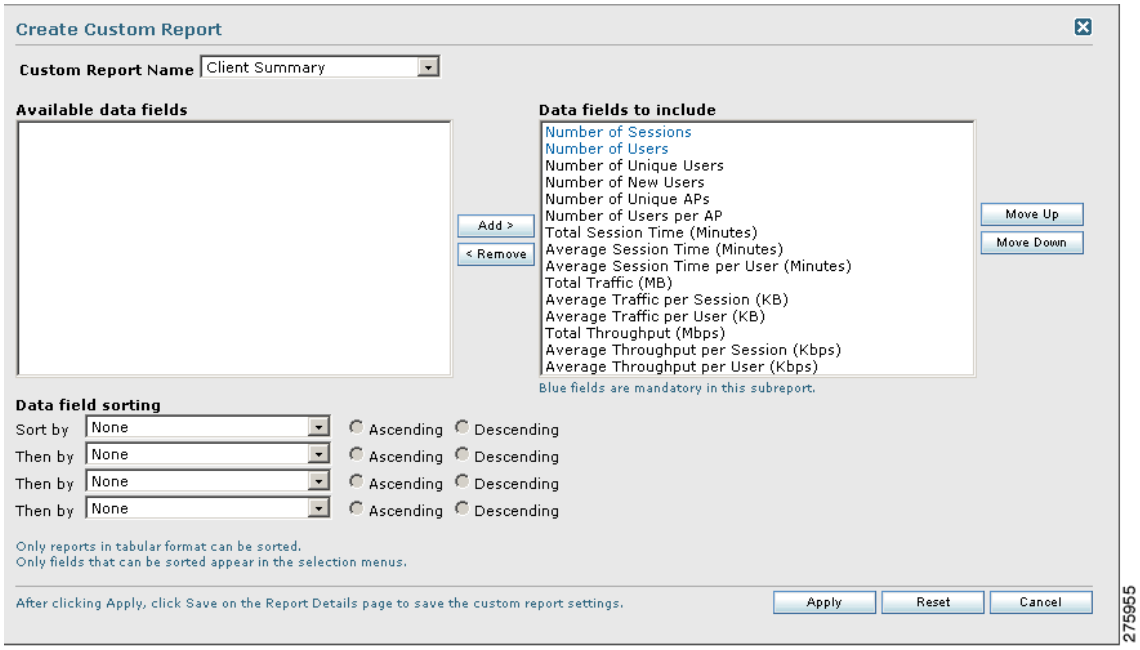
Report	Customizable	Multiple Sub-Reports?	Report Views	Report View Customizable?
New Rogue AP Count	No	No	Graphical	No
Rogue AP Events	Yes	No	Tabular	No
Rogue APs	Yes	No	Tabular	No
Security Summary	Yes	No	Tabular	No

[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 (similar to other inventory reports: APs/Controllers/MSEs) consists of multiple sub-reports. 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 17-4).

Figure 17-4 Customize Report View Page



Create Custom Report

Custom Report Name: Client Summary

Available data fields

Data fields to include:
Number of Sessions
Number of Users
Number of Unique Users
Number of New Users
Number of Unique APs
Number of Users per AP
Total Session Time (Minutes)
Average Session Time (Minutes)
Average Session Time per User (Minutes)
Total Traffic (MB)
Average Traffic per Session (KB)
Average Traffic per User (KB)
Total Throughput (Mbps)
Average Throughput per Session (Kbps)
Average Throughput per User (Kbps)

Blue fields are mandatory in this subreport.

Data field sorting
Sort by: None ○ Ascending ○ Descending
Then by: None ○ Ascending ○ Descending
Then by: None ○ Ascending ○ Descending
Then by: None ○ Ascending ○ Descending

Only reports in tabular format can be sorted.
Only fields that can be sorted appear in the selection menus.

After clicking Apply, click Save on the Report Details page to save the custom report settings.

a. From the Custom Report Name drop-down list, select the report you intend to run. 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 panels (Available data fields and Data fields to include).

Note Column headings in blue are mandatory in the current subreport. 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 select each data field for sorting.
   - For each sorted data field, select 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.

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 from 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 Now—Click to run the report without saving the report setup.
- 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.

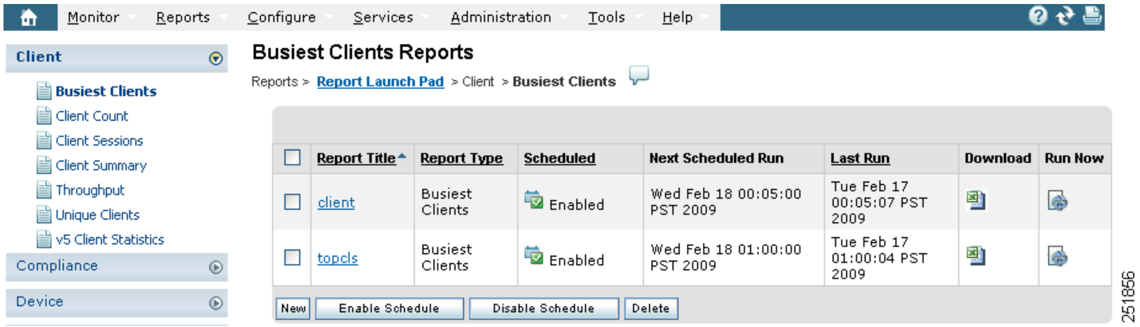
To access current or saved reports from the Report Launch Pad, follow these steps:

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 17-5).

Note To view a list of saved reports, choose **Reports > Saved Reports**. See the "Managing Saved Reports" section on page 17-11 for more information.

Figure 17-5 Current Reports Page



Busiest Clients Reports

Reports > Report Launch Pad > Client > Busiest Clients

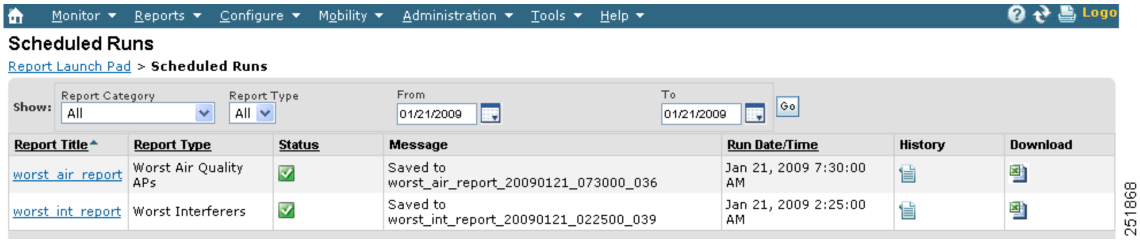
☐	Report Title	Report Type	Scheduled	Next Scheduled Run	Last Run	Download	Run Now
☐	client	Busiest Clients	Enabled	Wed Feb 18 00:05:00 PST 2009	Tue Feb 17 00:05:07 PST 2009		
☐	topcls	Busiest Clients	Enabled	Wed Feb 18 01:00:00 PST 2009	Tue Feb 17 01:00:04 PST 2009		

Managing Scheduled Run Results

To view all currently scheduled runs in WCS, choose **Report > Scheduled Run Results** (see Figure 17-6).

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

Figure 17-6 Scheduled Run Results Page



Scheduled Runs

Report Launch Pad > Scheduled Runs

Show: Report Category All Report Type All From 01/21/2009 To 01/21/2009

Report Title	Report Type	Status	Message	Run Date/Time	History	Download
worst_air_report	Worst Air Quality APs	✓	Saved to worst_air_report_20090121_073000_036	Jan 21, 2009 7:30:00 AM		
worst_int_report	Worst Interferers	✓	Saved to worst_int_report_20090121_022500_039	Jan 21, 2009 2:25:00 AM		

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.

Select one of the following links for additional information on scheduled run results:

- Sorting Scheduled Run Results
- Viewing or Editing Scheduled Run Details

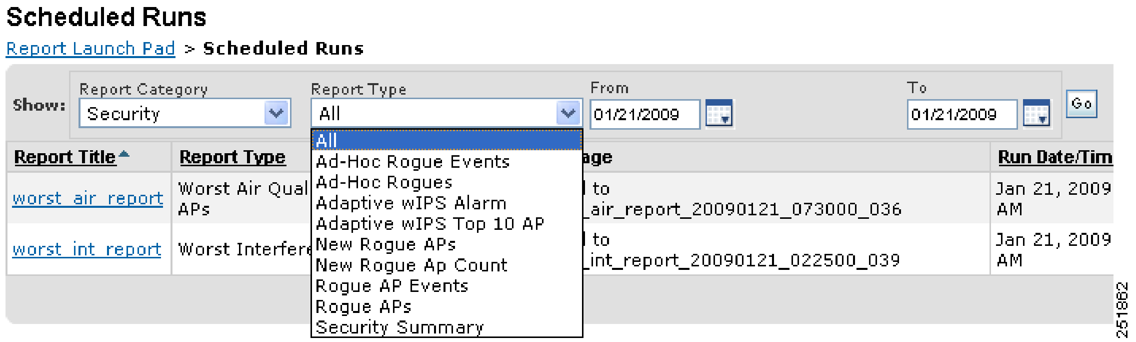
Sorting Scheduled Run Results

You can use the Show drop-down lists to sort the Scheduled Run Results by category, type, and time frame (see Figure 17-7):

- Report Category—Select the appropriate report category from the drop-down list or select **All**.
- Report Type—Select the appropriate report type from the drop-down list or select **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 17-7 Sorting Scheduled Run Results



Scheduled Runs

Report Launch Pad > **Scheduled Runs**

Show: Report Category: Security | Report Type: All | From: 01/21/2009 | To: 01/21/2009 | Go

Report Title	Report Type	age	Run Date/Tim
worst_air_report	Worst Air Qual APs	to air_report_20090121_073000_036	Jan 21, 2009 AM
worst_int_report	Worst Interfere	to int_report_20090121_022500_039	Jan 21, 2009 AM

Viewing or Editing Scheduled Run Details

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

Step 1 Select **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:

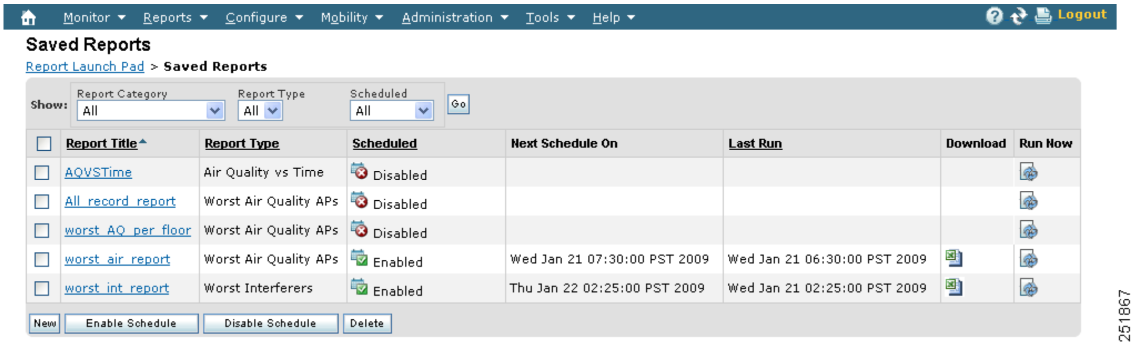
- Save—Click to save this schedule run without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this scheduled run and to immediately run the report.
- Cancel—Click to return to the previous page without running nor saving this report.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

Managing Saved Reports

In the Saved Reports page, you can create and manage saved reports (see Figure 17-8). To open this page in WCS, choose **Reports > Saved Reports**.

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

Figure 17-8 Saved Reports Page



Saved Reports

Report Launch Pad > Saved Reports

Show: Report Category: All | Report Type: All | Scheduled: All | Go

☐	Report Title ▴	Report Type	Scheduled	Next Schedule On	Last Run	Download	Run Now
☐	AQVSTime	Air Quality vs Time	Disabled				▶
☐	All_record_report	Worst Air Quality APs	Disabled				▶
☐	worst_AQ_per_floor	Worst Air Quality APs	Disabled				▶
☐	worst_air_report	Worst Air Quality APs	Enabled	Wed Jan 21 07:30:00 PST 2009	Wed Jan 21 06:30:00 PST 2009	⬇	▶
☐	worst_int_report	Worst Interferers	Enabled	Thu Jan 22 02:25:00 PST 2009	Wed Jan 21 02:25:00 PST 2009	⬇	▶

New | Enable Schedule | Disable Schedule | Delete

The Saved Reports 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.
- Next Schedule On—Indicates the date and time of the next scheduled run for this report.
- Last Run—Indicates the date and time of the most recent scheduled run for this report.
- Download—Click the **Download** icon to open or save a .csv file of the report results.
- Run Now—Click the **Run Now** icon to immediately run the current report.

Select one of the following links for additional information on saved reports:

- Sorting Saved Reports
- Viewing or Editing Saved Report Details
- Running a Saved Report

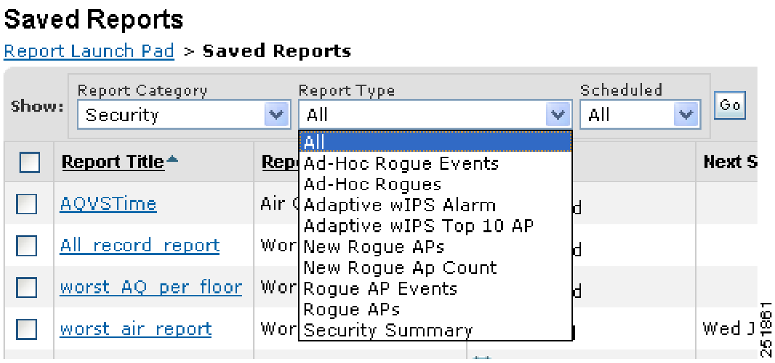
Sorting Saved Reports

You can use the Show drop-down lists to sort the Saved Reports list by category, type, and scheduled status (see Figure 17-9).

- Report Category—Select the appropriate report category from the drop-down list or select **All**.

- Report Type—Select the appropriate report type from the drop-down list or select **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Select **All**, **Enabled**, **Disabled**, or **Expired** to sort the Saved Reports list by scheduled status.

Figure 17-9 Sorting Saved Reports



Saved Reports

Report Launch Pad > Saved Reports

Show: Report Category: Security; Report Type: All; Scheduled: All

□	Report Title	Rep		Next S
□	AQVSTime	Air (	d	
□	All record report	Wor	d	
□	worst AQ per floor	Wor	d	
□	worst air report	Wor		Wed J

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

Viewing or Editing Saved Report Details

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

Step 1 Select **Report > Saved Reports**.

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.

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 Now—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.

Running a Saved Report

In the Reports > Saved Reports page, click **Run Now** for the appropriate report.

Specific WCS Reports

- 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 Stream Metrics
  - Unique Clients
  - V5 Client Statistics
- Compliance Reports
  - Configuration Audit
  - Payment Card Industry (PCI)
- Device Reports
  - AP Profile Status
  - Busiest APs
  - AP Summary
  - Inventory Reports
  - Uptime
  - Utilization
- Guest Reports
  - Guest Accounts Status
  - Guest Association
  - Guest Count
  - Guest User Sessions
  - WCS Guest Operations
- Mesh Reports
  - Alternate Parent
  - Link Stats
  - Nodes
  - Packet Stats
  - 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 Alarms
  - Adaptive wIPS Top 10 Access Points
  - Adhoc Rogue Events
  - Adhoc Rogues
  - New Rogue Access Points
  - New Rogue Access Point Count
  - Rogue Access Points Events
  - Rogue Access Points
  - Security Summary

CleanAir Reports

Click **New** for CleanAir report type to create a new report. See "Creating and Running a New Report" for more information.

Click a report type to view currently saved reports. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

The following are available 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. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

To create a new report, click **New** from the Report Launch Pad or from the Air Quality vs Time page. See "Configuring a AirQuality vs Time Report" and "Air Quality vs Time Report Results" for more information.

Configuring a AirQuality vs Time Report

Settings

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

- Report Title—If you plan to use this as a saved report, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Controllers > All Access Points** or click **Edit** to select specific access points.
  - AP By Floor Area—Choose **System Campus > All Access Points** or click **Edit** to select specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to select 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. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed in each page.

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 "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" 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 Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" 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 "Creating and Running a New Report" for more information on customizing report results.

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

- AP Name
- Basic Radio MAC
- 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 reports. See "Managing Current Reports" for more information.

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

Configuring 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, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP By Floor Area—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to select 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. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed on each page.

  Note 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 "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" 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 Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" 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 "Creating and Running a New Report" 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 reports. See "Managing Current Reports" for more information.

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

Configuring 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, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP By Floor Area—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click Edit to select 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. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed on each page.

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 "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" 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 Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" 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 "Creating and Running a New Report" 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 reports. See "Managing Current Reports" 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

Settings

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

- Report Title—If you plan to use this as a saved report, 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 select specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Area** from the report criteria area or click **Edit** to select 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. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed on each page.

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 "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" 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 Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" 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 "Creating and Running a New Report" 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, 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
- Client Traffic Stream Metrics
- Unique Clients
- V5 Client Statistics

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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select 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 select specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page or click **Edit** to select 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—Select **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. Select 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 17-2 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 17-2 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 includes:

- 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 17-2 for more information on customizing report results.

The following potential results occur, depending on how the report is customized. See Figure 17-10 for potential results for the Busiest Client report.

- 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.

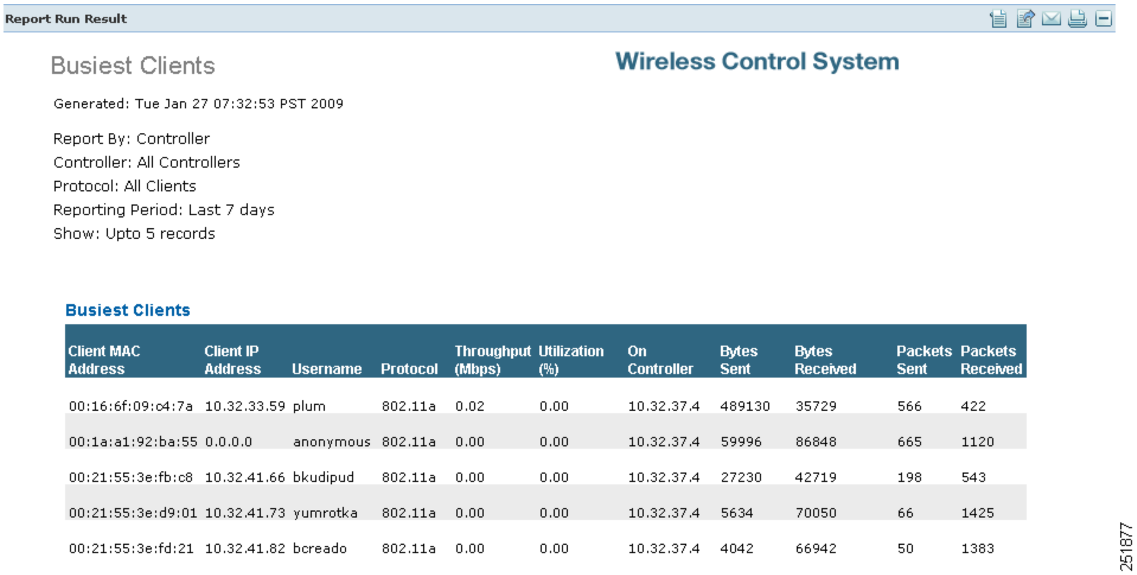
- Utilization (%)
- On Controller—The controller on which the client is located.
- Bytes sent and received

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 17-10 Busiest Client Report Results



Busiest Clients

Generated: Tue Jan 27 07:32:53 PST 2009

Report By: Controller
Controller: All Controllers
Protocol: All Clients
Reporting Period: Last 7 days
Show: Upto 5 records

Busiest Clients

Client MAC Address	Client IP Address	Username	Protocol	Throughput (Mbps)	Utilization (%)	On Controller	Bytes Sent	Bytes Received	Packets Sent	Packets Received
00:16:6f:09:c4:7a	10.32.33.59	plum	802.11a	0.02	0.00	10.32.37.4	489130	35729	566	422
00:1a:a1:92:ba:55	0.0.0.0	anonymous	802.11a	0.00	0.00	10.32.37.4	59996	86848	665	1120
00:21:55:3e:fb:c8	10.32.41.66	bkudipud	802.11a	0.00	0.00	10.32.37.4	27230	42719	198	543
00:21:55:3e:d9:01	10.32.41.73	yumrotka	802.11a	0.00	0.00	10.32.37.4	5634	70050	66	1425
00:21:55:3e:fd:21	10.32.41.82	bcreado	802.11a	0.00	0.00	10.32.37.4	4042	66942	50	1383

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.

This report contains the following settings and scheduling parameters:

Settings

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

- Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
- Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
- Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
- AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
- AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
- SSID—Select **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
- AP by RAP Mesh Role—Select **All RAP APs** from the Report Criteria page or click **Edit** to select 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—Select **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. Select 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 17-2 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 17-2 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 includes:

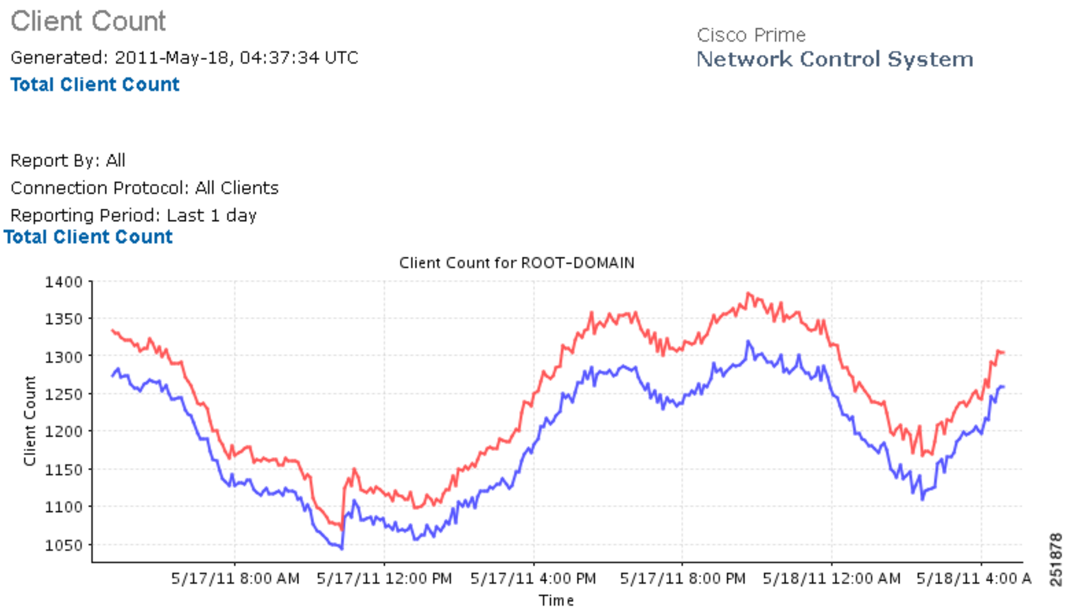
- Controller IP—The IP address of the controller.
- Time—The time the client count occurred.
- Associated Client Count—The number of associated clients for the specified period of time.
- Authenticated Client Count—The number of authenticated clients for the specified period of time.

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 17-2 for more information on customizing report results.

The Client Count report displays the following graph for the results (Figure 17-11):

Figure 17-11 Client Count Report Results



Client Count

Generated: 2011-May-18, 04:37:34 UTC

Total Client Count

Cisco Prime
Network Control System

Report By: All

Connection Protocol: All Clients

Reporting Period: Last 1 day

Total Client Count

Client Sessions

This report displays the clients on the network, client statistics, and the access points to which they are connected.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - SSID—Select **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Select **All RAP APs** from the Report Criteria page or click **Edit** to select 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. Select 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 "Creating and Running a New Report" section on page 17-2 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 17-2 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 includes:

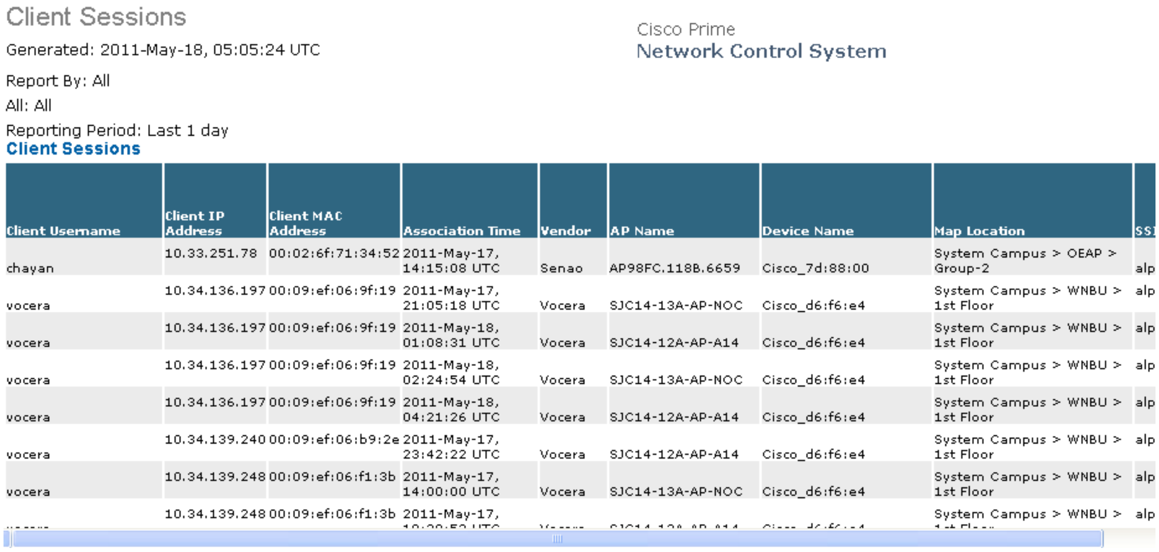
- Client Username
- Client IP Address—The IP address of the client.
- Client MAC Address—The MAC address of the client.
- Association Time —The date and time the client associated.
- Vendor—The vendor name for this client.
- AP Name—The access point to which this client is associated.
- Controller Name—The 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. WCS does a DNS lookup to resolve the host name from the client's IP address. 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 17-2 for more information on customizing report results.

The following image (Figure 17-12) displays potential results for the Client Sessions report, depending on how the report is customized:

Figure 17-12 Client Sessions Report Results



Client Sessions

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

Cisco Prime
Network Control System

Report By: All

All: All

Reporting Period: Last 1 day

Client Sessions

Client Username	Client IP Address	Client MAC Address	Association Time	Vendor	AP Name	Device Name	Map Location	SSI
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	alp
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	alp
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	alp
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	alp
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	alp
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	alp
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	alp
	10.34.139.248	00:09:ef:06:f1:3b	2011-May-17,				System Campus > WNBU >	alp

Client Summary

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

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, 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. Select 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 17-2 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 17-2 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 includes summary results sorted by protocol, SSID, VLAN, and vendor. To customize report results for a particular section, select 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 information 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 WCS does not receive client traps, it relies on client status polling to discover client associations (The task runs every 5 minutes by default.). However, WCS cannot accurately determine when the client was actually associated. WCS 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

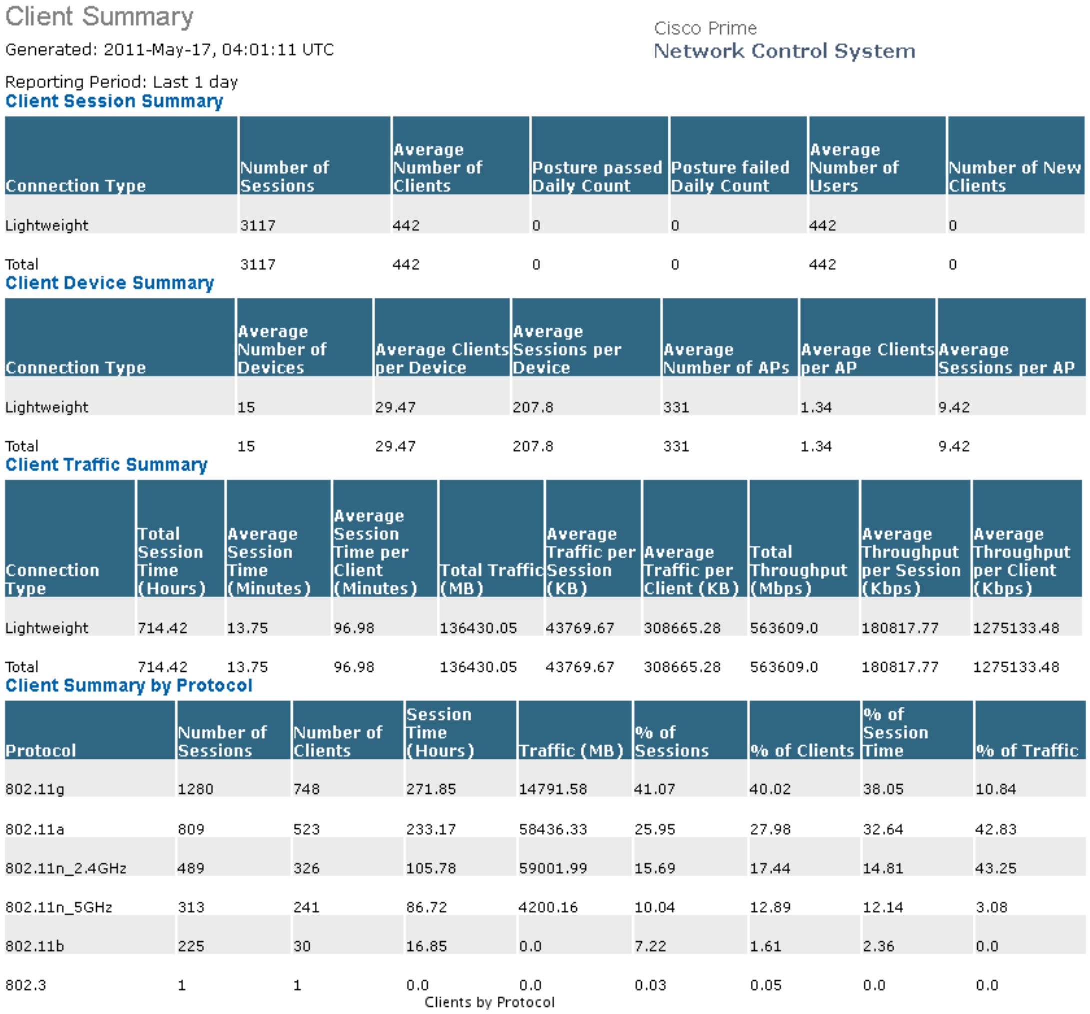
- Time Used (Minutes)
- Traffic (MB)
- Session Count
- % of Users
- % of Time
- % of Traffic
- % of Session
- Total Time of a session

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 17-2 for more information on customizing report results.

The Client Summary report contains the following potential results (see Figure 17-13), depending on how the report is customized:

Figure 17-13 Client Summary Report Results



Client Summary

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

Reporting Period: Last 1 day

Cisco Prime
Network Control System

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 Stream Metrics

The Client Traffic Stream Metrics report displays client or SSID based traffic stream metric (TSM) information.

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 reports. See the "Managing Current Reports" section on page 17-8 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.

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, enter a report name.
- Report by
  - SSID—Choose **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - Client MAC Address—Choose **All Clients** from the Report Criteria page or click **Edit** to select 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. Select 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 17-2 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 17-2 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 17-2 for more information on customizing report results.

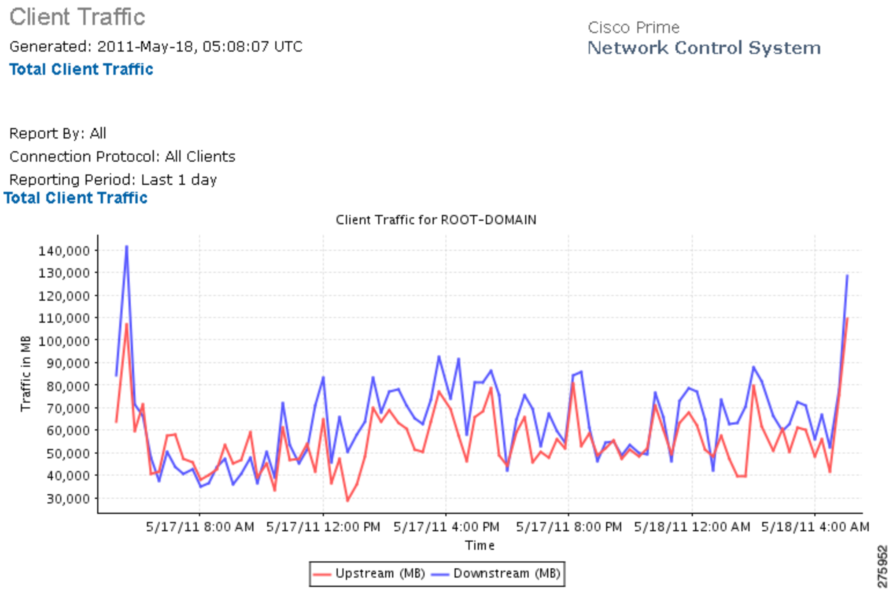
The following are potential results for a Client Traffic Stream Metrics report, depending on how the report is customized:

- 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

The Client Traffic Stream Metrics Report contains the following results (see Figure 17-14).

Figure 17-14 Client Traffic Stream Metrics Report Results



Client Traffic

Generated: 2011-May-18, 05:08:07 UTC

Total Client Traffic

Cisco Prime
Network Control System

Report By: All

Connection Protocol: All Clients

Reporting Period: Last 1 day

Total Client Traffic

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.

This report displays the following settings and scheduling parameters:

Settings

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

- Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
- AP by Controller—Select **All Controllers > All Access Points** or click **Edit** to select specific devices.
- AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
- AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
- Criteria page or click **Edit** to select 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—Select **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. Select 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.

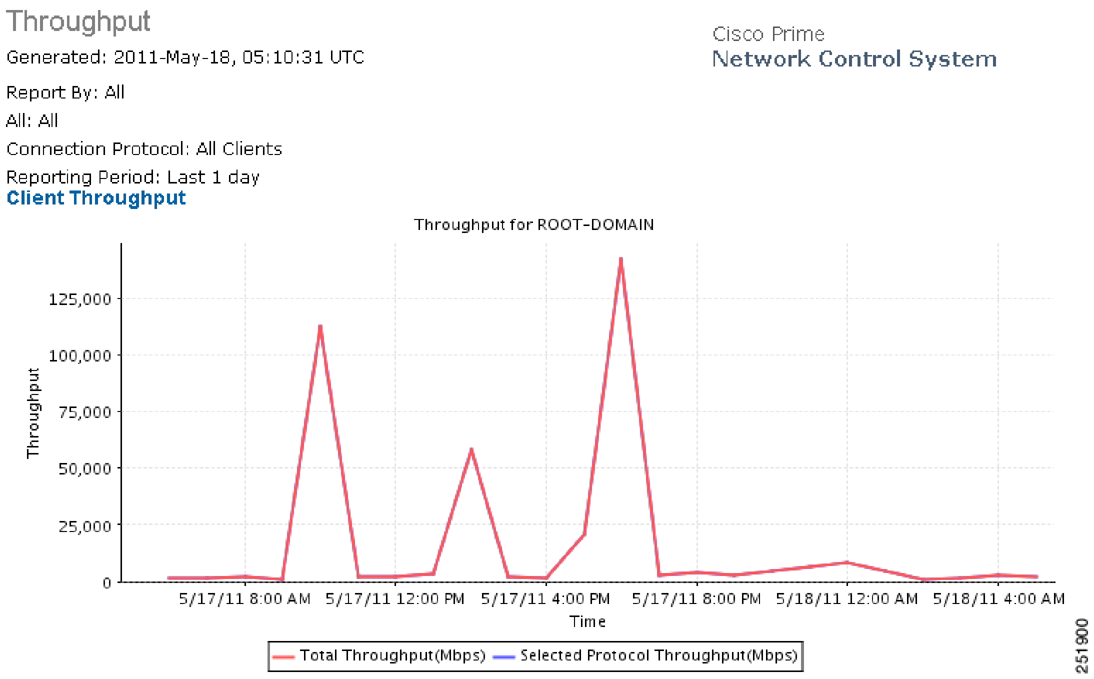
Schedule

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 17-2 for more information on scheduling a report.

Throughput Report Results

The Throughput report displays the following results (Figure 17-15):

Figure 17-15 Throughput Report Results



Throughput

Generated: 2011-May-18, 05:10:31 UTC

Report By: All

All: All

Connection Protocol: All Clients

Reporting Period: Last 1 day

Client Throughput

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.

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

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

This report displays the following settings and scheduling parameters:

Settings

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

  - Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - SSID—Select **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Select **All RAP APs** from the Report Criteria page or click **Edit** to select a specific RAP access point.
  - Select 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—Select **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. Select 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 17-2 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 17-2 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:

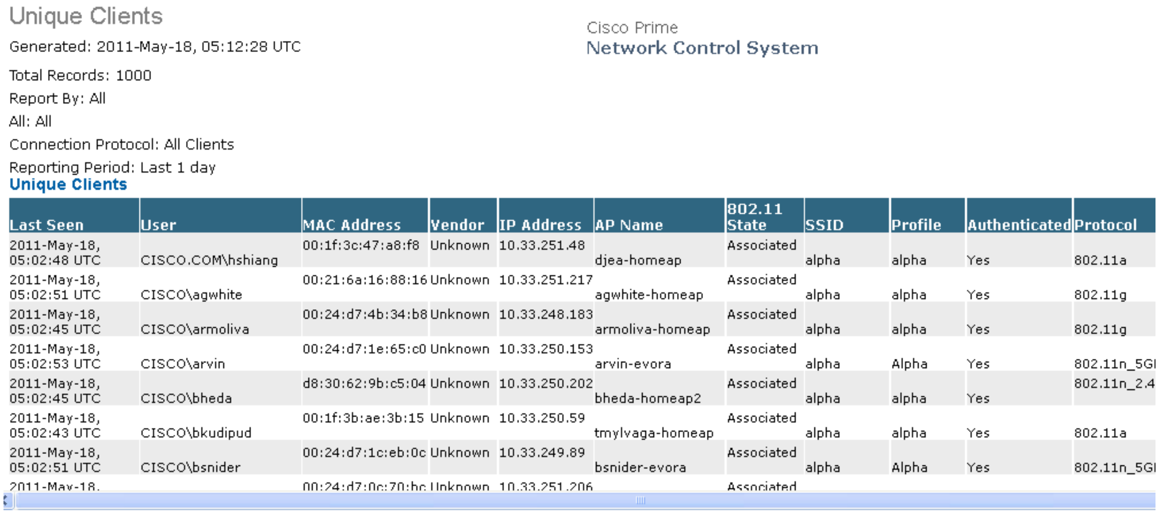
- Host Name
- AP MAC Address

- 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 results appear for the Throughput report (Figure 17-16):

Figure 17-16 Unique Client Report Results



Unique Clients

Cisco Prime
Network Control System

Generated: 2011-May-18, 05:12:28 UTC

Total Records: 1000
Report By: All
All: All
Connection Protocol: All Clients
Reporting Period: Last 1 day

Unique Clients

Last Seen	User	MAC Address	Vendor	IP Address	AP Name	802.11 State	SSID	Profile	Authenticated	Protocol
2011-May-18, 05:02:48 UTC	CISCO.COM\hshiang	00:1f:3c:47:a8:f8	Unknown	10.33.251.48	djea-homeap	Associated	alpha	alpha	Yes	802.11a
2011-May-18, 05:02:51 UTC	CISCO\agwhite	00:21:6a:16:88:16	Unknown	10.33.251.217	agwhite-homeap	Associated	alpha	alpha	Yes	802.11g
2011-May-18, 05:02:45 UTC	CISCO\armoliva	00:24:d7:4b:34:b8	Unknown	10.33.248.183	armoliva-homeap	Associated	alpha	alpha	Yes	802.11g
2011-May-18, 05:02:53 UTC	CISCO\arvin	00:24:d7:1e:65:c0	Unknown	10.33.250.153	arvin-evora	Associated	alpha	Alpha	Yes	802.11n_5G
2011-May-18, 05:02:45 UTC	CISCO\bheda	d8:30:62:9b:c5:04	Unknown	10.33.250.202	bheda-homeap2	Associated	alpha	alpha	Yes	802.11n_2.4
2011-May-18, 05:02:43 UTC	CISCO\bkudipud	00:1f:3b:ae:3b:15	Unknown	10.33.250.59	tmylvaga-homeap	Associated	alpha	alpha	Yes	802.11a
2011-May-18, 05:02:51 UTC	CISCO\bsnider	00:24:d7:1c:eb:0c	Unknown	10.33.249.89	bsnider-evora	Associated	alpha	Alpha	Yes	802.11n_5G
2011-May-18,		00:24:d7:0c:70:bc	Unknown	10.33.251.206		Associated				

V5 Client Statistics

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

This report displays the following settings and scheduling parameters:

Settings

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

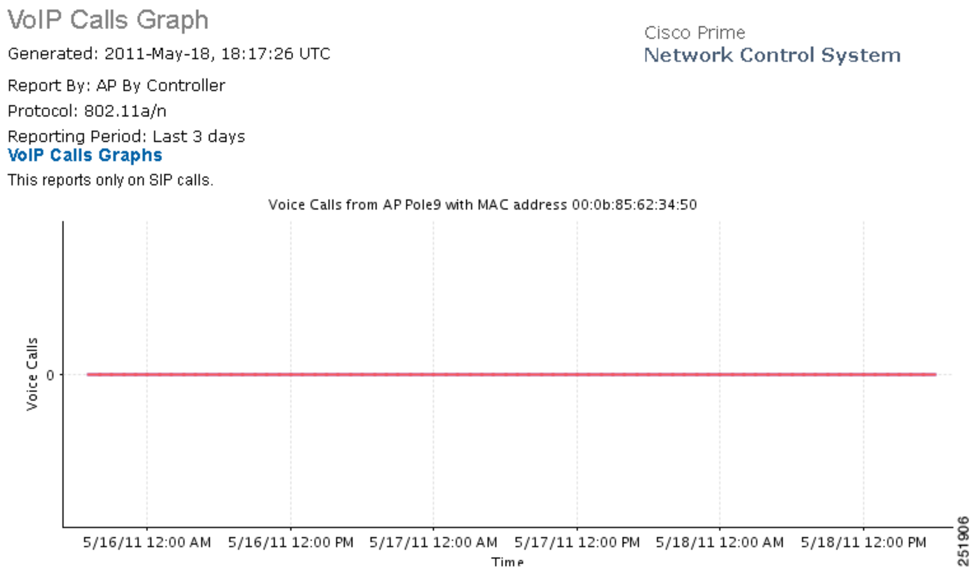
Schedule

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 17-2 for more information on scheduling a report.

V5 Client Statistics Report Results

This report displays the following results for the v5 Client Statistics report (Figure 17-17):

Figure 17-17 V5 Client Statistics Report Results



VoIP Calls Graph

Generated: 2011-May-18, 18:17:26 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

VoIP Calls Graphs

This reports only on SIP calls.

Compliance Reports

The Configuration Audit report displays the differences between WCS 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 https://www.pcisecuritystandards.org.

- Configuration Audit
- Payment Card Industry (PCI)

Configuration Audit

This report displays the configuration differences between WCS 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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Controller—Select **All Controllers** or a specific controller from the available list.
- Audit Time—Select **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. Select 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 17-2 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 17-2 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 includes the following sections: Audit Summary, Applied Templates and Config Group Template Discrepancies, Enforced Values, Failed Enforcements, and WCS Config Discrepancies. Select the applicable report from the Customizable Report drop-down list.
To customize report results for a particular section, select the applicable section from the Customizable Report drop-down list.

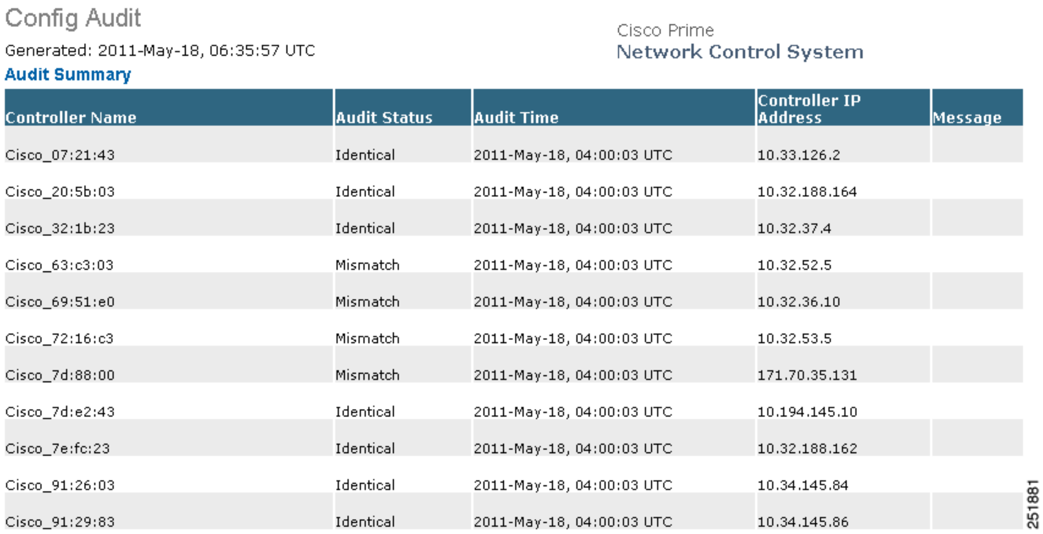
A Configuration Audit report contains the following default information, depending on which customized report is selected:

- 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 WCS
- Attribute Value in Device
- Enforced Value
- Instance Name
- Description
- Error Message
- Attribute Value in DB

Configuration Audit Results

The Configuration Audit report contains the following results (Figure 17-18):

Figure 17-18 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	

Payment Card Industry (PCI)

This report displays the PCI Data Security Standard (DSS) version 1.1 requirements that are relevant to your wireless network security.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, 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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

Note A PCI report includes the following sections: New Rogue APs, Adhoc Rogues, Config Compliance, Location Server/Mobility Service Engine, Auth Enc Violations, Client Association, Access Points, Controllers, Autonomous Access Points, MSEs, and Threats and Attacks.
To customize report results for a particular section, select the appropriate section from the Customizable Report drop-down list.

New Rogue APs report results include:

- Created Time
- Rogue MAC Address
- Detecting AP Name
- Radio Type
- Controller IP Address
- SSID—The user-defined Service Set Identifier name.
- State
- Map Location—The building, floor area, or outdoor area (as applicable) where the new rogue access point is located.
- Channel Number
- RSSI (dBm)
- Classification Type

Adhoc Rogues report results include:

- Modified Time
- Rogue MAC Address
- Detecting AP Name
- Radio Type
- Controller IP Address
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue is located.
- SSID—The user-defined Service Set Identifier name.
- Channel Number

- RSSI (dBm)
- State

Config Compliance, Location Server/ Mobility Services Engine, and Auth Enc Violations report results include:

- IP Address
- Device Security Issues
- Device Name
- Device Type—Indicates the device type as MSE 3310, MSE 3350, or 2710 Location Server.

Client Association report results include:

- Time
- Client MAC Address—The MAC address of the client.
- Controller IP Address
- AP Name—The access point name.
- Client Username
- Status
- Session Duration
- Reason

Access Point report results include:

- AP Name—The access point name.
- Ethernet MAC Address
- IP Address
- Model
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name
- Base radio MAC Address
- Software Version
- Detailed Location
- Primary Controller
- Secondary Controller Name
- Tertiary Controller Name
- Admin Status
- AP Mode
- 802.11a/n Status
- 802.11b/g/n Status
- Gateway
- Netmask
- IOS version

- Boot version
- Certificate type
- Serial number
- Local interface
- Neighbor name
- Neighbor address
- Neighbor port
- Neighbor Advt version

Controller report results include:

- Controller name
- Location
- Model
- Reachability status
- IP address
- Serial number
- Software version
- Mobility group

Autonomous Access Point reports results include:

- AP Name—The access point name.
- Ethernet MAC address
- Model
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Reachability status
- 802.11a/n MAC address
- 802.11b/g/n MAC address
- IP address—The IP address of the MSE or Location Server.
- Software version
- Location
- 802.11a/n status
- 802.11b/g/n status
- Serial number

MSE report results include:

- Device name
- Start time—The start time of the MSE or Location Server.
- HTTP/HTTPS port—The port numbers for HTTP and HTTPS.
- HTTPS—Whether HTTPS is enabled or disabled.
- Version

- IP address
- Device type

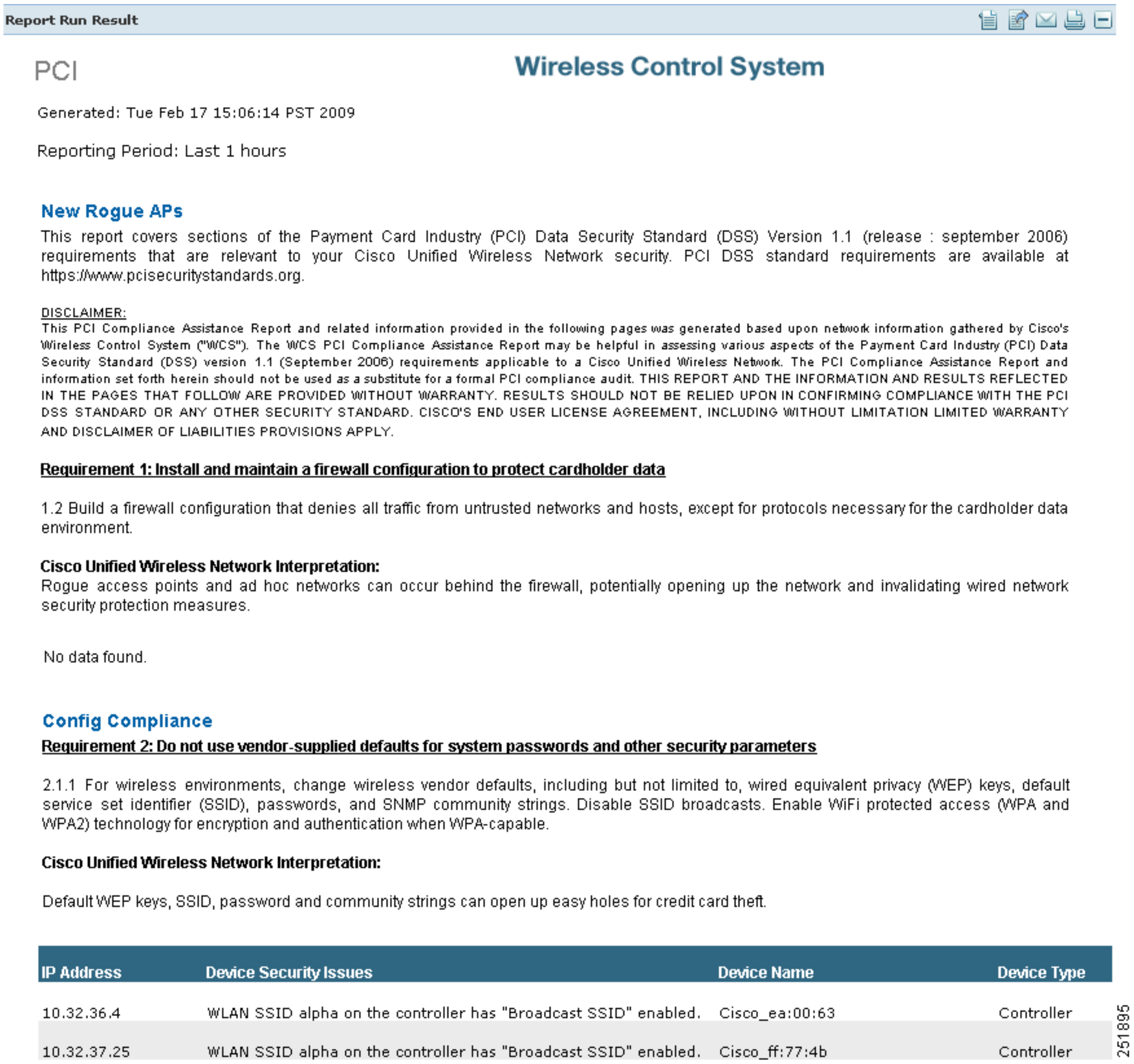
Threats and Attacks report results include:

- Severity
- Date/Time
- Message
- Failure Object

PCI Report Results

The PCI report contains the following results (Figure 17-19):

Figure 17-19 PCI Report Results



Report Run Result

PCI

Wireless Control System

Generated: Tue Feb 17 15:06:14 PST 2009

Reporting Period: Last 1 hours

New Rogue APs

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.1 (release : september 2006) requirements that are relevant to your Cisco Unified Wireless Network security. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.

DISCLAIMER:
This PCI Compliance Assistance Report and related information provided in the following pages was generated based upon network information gathered by Cisco's Wireless Control System ("WCS"). The WCS PCI Compliance Assistance Report may be helpful in assessing various aspects of the Payment Card Industry (PCI) Data Security Standard (DSS) version 1.1 (September 2006) requirements applicable to a Cisco Unified Wireless Network. The PCI Compliance Assistance 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.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

1.2 Build a firewall configuration that denies all traffic from untrusted networks and hosts, except for protocols necessary for the cardholder data environment.

Cisco Unified Wireless Network Interpretation:
Rogue access points and ad hoc networks can occur behind the firewall, potentially opening up the network and invalidating wired network security protection measures.

No data found.

Config Compliance

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

Cisco Unified Wireless Network Interpretation:

Default WEP keys, SSID, password and community strings can open up easy holes for credit card theft.

IP Address	Device Security Issues	Device Name	Device Type
10.32.36.4	WLAN SSID alpha on the controller has "Broadcast SSID" enabled.	Cisco_ea:00:63	Controller
10.32.37.25	WLAN SSID alpha on the controller has "Broadcast SSID" enabled.	Cisco_ff:77:4b	Controller

Device Reports

You can create the following device reports:

- AP Image Predownload
- AP Profile Status
- Busiest APs
- AP Summary
- Inventory Reports
- 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 reports. See "Managing Current Reports" for more information.

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

Configuring 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, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select specific devices.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select specific locations or devices.

Note In the Report Criteria page, you can select **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 a number between 10 and 50, or leave blank to show all records.

Schedule

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

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See "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. 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 Now—Click to run the report without saving the report setup.
- 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 "Creating and Running a New Report" 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.

This report displays the following settings and scheduling parameters:

Settings

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

Note In the Reports Criteria page, you can select **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. Select 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 17-2 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 17-2 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:

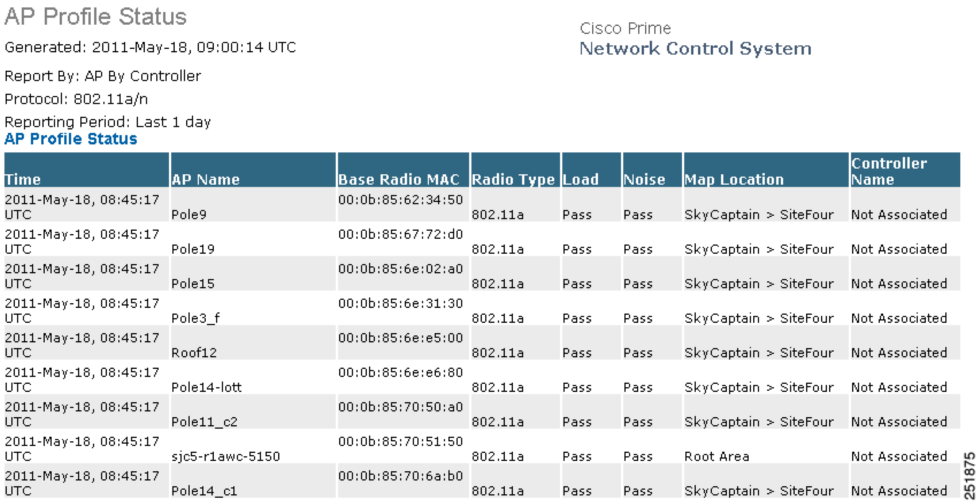
- Time—The date and time at which AP Profile Status is collected.
- AP Name—The access point name.
- AP MAC address—The MAC address of the access point.

- 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 AP Profile Status report contains the following results (Figure 17-20):

Figure 17-20 AP Profile Status Report Results



AP Profile Status

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

Cisco Prime
Network Control System

Report By: AP By Controller
Protocol: 802.11a/n
Reporting Period: Last 1 day

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

Busiest APs

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

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Protocol—Select 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. Select 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 on each page.

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 17-2 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 17-2 for more information on customizing report results.

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

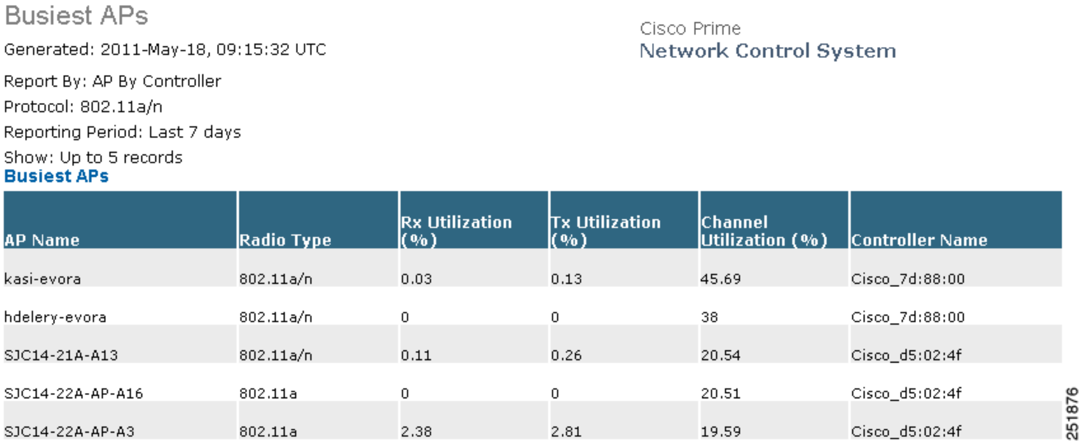
Busiest APs report results include:

- 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 Busiest APs report contains the following results (Figure 17-21):

Figure 17-21 Busiest APs Report Results



Busiest APs

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

Cisco Prime
Network Control System

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

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

AP Summary

This report displays the distribution of devices on your wireless network. This report enables you to sort the devices by RF group name, mobility group name, access point group name, SSID, location, and other statistics.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Floor Area—Select **All Campuses** > **All Builders** > **All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Select **All Campuses** > **All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - OfficeExtend AP—Select **Enable** from the Report Criteria page or click **Edit** to select **Enable** or **Disable**.
  - AP by Controller—Select **All Controllers** > **All APs** from the Report Criteria page or click **Edit** to select specific devices.
  - AP Group—Select **All AP Groups** from the Report Criteria page or click **Edit** to select a specific access point group.
  - RF Group—Select **All RF Groups** from the Report Criteria page or click **Edit** to select a specific radio frequency group.
  - AP Mode—Select **All AP Modes** from the Report Criteria page or click **Edit** to select 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—Select 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 17-2 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 17-2 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:

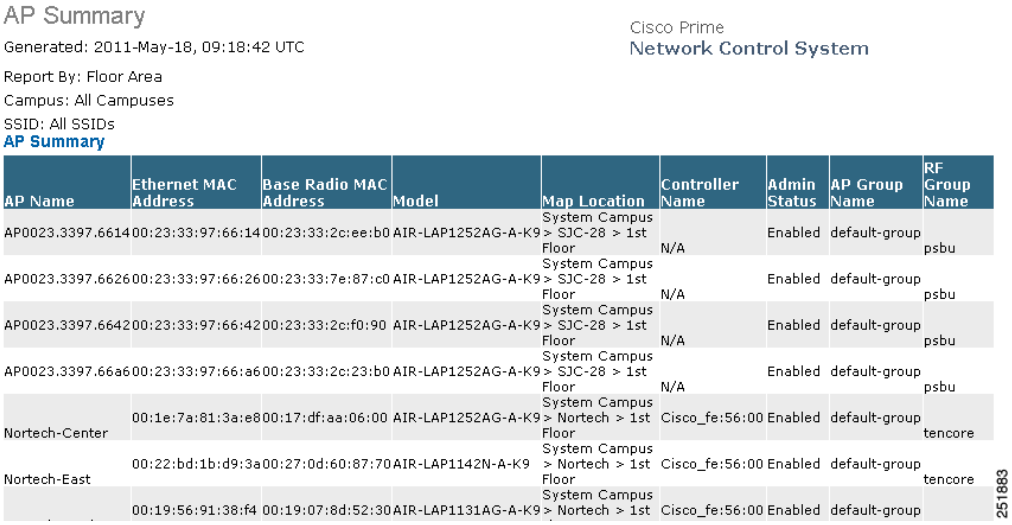
- AP Name—The access point name.
- Ethernet MAC Address
- Base radio MAC Address
- Model
- Location
- Primary Controller
- Admin Status—Enable/Disable.
- AP group Name
- RF group Name
- Software Version

- 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 Summary Report Results

The AP Summary report contains the following results (Figure 17-22):

Figure 17-22 AP Summary Report Results - NEED SCREENSHOT WITH AP SUMMARY



AP Summary

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

Report By: Floor Area

Campus: All Campuses

SSID: All SSIDs

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	

Inventory Reports

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

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Choose **Combined Inventory**, **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 17-2 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 17-2 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 includes the following sections: Count of Controllers by Model, Count of Controllers by Software Version, Controller Inventory, Count of APs by Model, Count of APs by Software Version.
To customize report results for a particular section, select the appropriate section from the Customizable Report drop-down list.

Available information for Count of Controllers by Model results includes:

- 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 includes:

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

Available information for Controller Inventory results includes:

- 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 CDP neighbor interface's duplex mode.

Available information for Count of APs by Model results includes:

- 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 includes:

- 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 includes:

- 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 access point's IP address.
- 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 access point's CDP neighbor's name, IP address, port, and advertised version information.

Available information for Count of MSEs by Version results includes:

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

Available information for MSEs results includes:

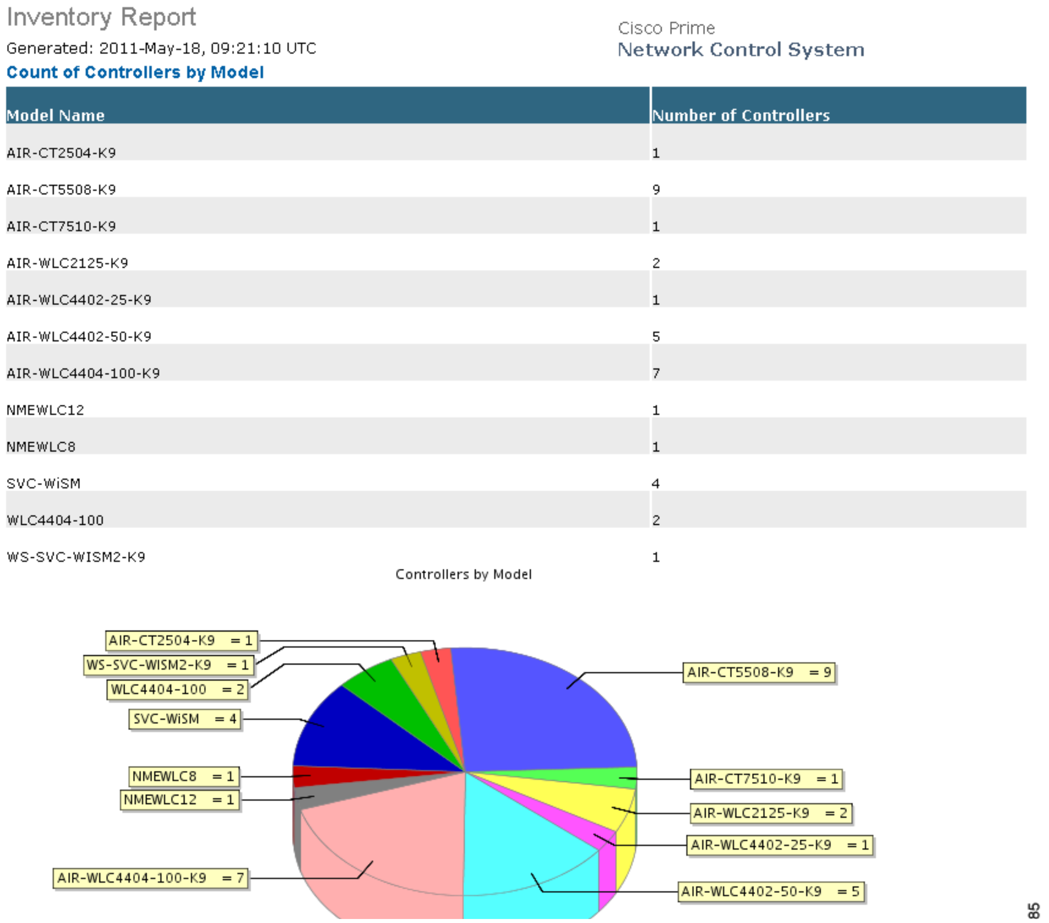
- Device Name—The name of the MSE or Location Server.
- IP Address
- Device Type

- HTTP/HTTPS Port
- HTTPS
- Version
- Start Time

Inventory Report Results

The following is an example of Inventory report results (Figure 17-23):

Figure 17-23 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.

This report displays the following settings and scheduling parameters:

Settings

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

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 17-2 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 17-2 for more information on customizing report results.

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

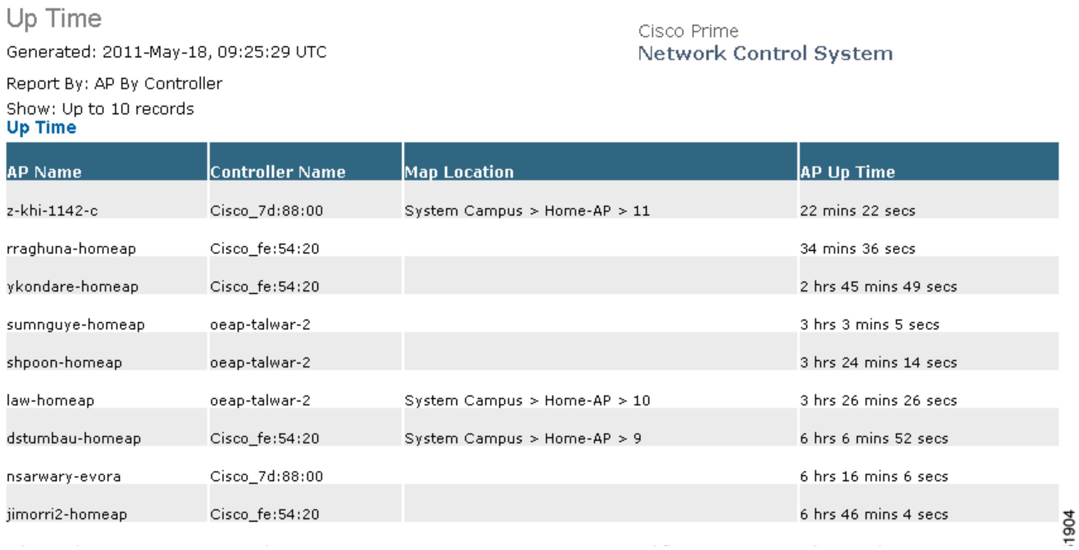
Available information for Uptime report results includes:

- 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 Uptime report displays the following results (Figure 17-24):

Figure 17-24 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

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 you monitor performance and plan for future expansion.

This report display the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Controllers**, **MSEs**, or **Radios** from the drop-down list.
- Report by (Report by options change depending on the report type selected)
  - Controller—If the report type is Controllers, select **All Controllers** from the Report Criteria page or click **Edit** to select 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 17-61.
  - MSEs—If the report type is MSEs, select **All MSEs** from the Report Criteria page or click **Edit** to select 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 17-61.
  - Radios—If the report type is Radio, select **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 select 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 17-61.

Note In the Radios Report Criteria page, you can select **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. Select 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 selected, 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.

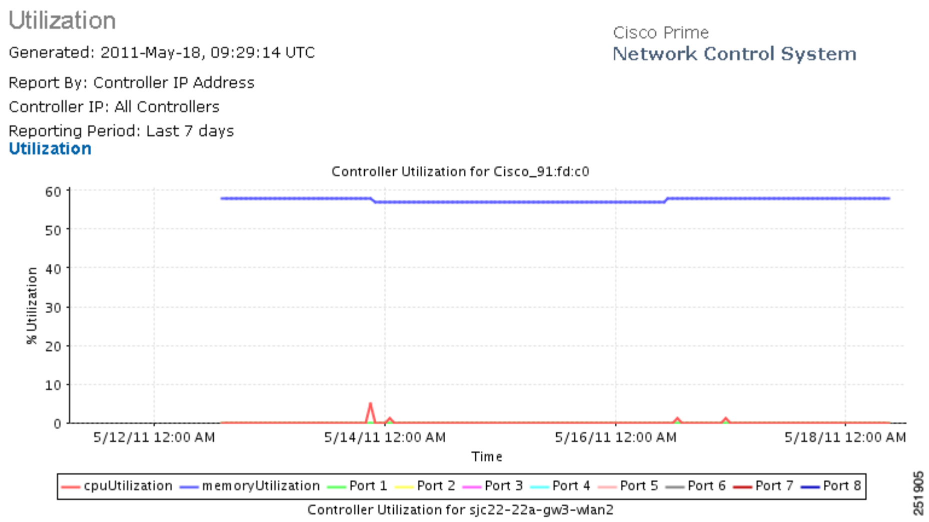
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Utilization Report Results

The Utilization report displays the following results (Figure 17-25):

Figure 17-25 Utilization Report Results



Utilization

Generated: 2011-May-18, 09:29:14 UTC

Report By: Controller IP Address

Controller IP: All Controllers

Reporting Period: Last 7 days

Cisco Prime
Network Control System

Utilization

Guest Reports

You can create the following guest reports:

- Guest Accounts Status
- Guest Association
- Guest Count
- Guest User Sessions
- WCS 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.

This report displays the following settings and scheduling parameters:

Settings

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

- WCS User—Select **All WCS Users** from the Report Criteria page or click **Edit** to select a specific WCS 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. Select 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 17-2 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 17-2 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 includes:

- 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.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Guest Profile—Select **All Profiles** from the Report Criteria page or click **Edit** to select a specific profile.
  - 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. Select 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 17-2 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 17-2 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 includes:

- 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.

This report display the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Guest Profile—Select **All Profiles** from the Report Criteria page or click **Edit** to select 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. Select 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 17-2 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 is configured from the Administration > Background Tasks page. This report is generated for guest users who are associated to controllers running software version 5.2 or above.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Guest User—Select **All Guest Users** from the Report Criteria page or click **Edit** to select 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 17-2 for more information on scheduling a report.

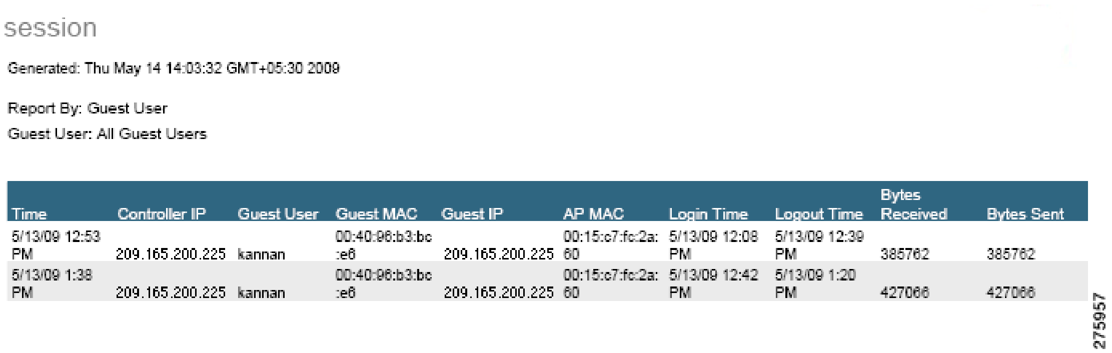
Guest User Sessions Report Results

The Guest User Sessions report contains the following information (refer to Figure 17-26):

- Controller IP Address
- Guest User
- Guest MAC Address

- Guest IP Address
- AP MAC
- Login Time
- Logout Time
- Bytes Received
- Bytes Sent

Figure 17-26 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

WCS 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 WCS, the activity performed by the deleted guest user still shows for up to one week after the activity occurred.

The following settings and scheduling parameters are available for this report:

Settings

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

Note All WCS 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. Select 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 17-2 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 17-2 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 includes:

- Time
- Reason
- WCS User
- Guest User
- Operation
- Status

WCS Guest Operation Report Results

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

- Time
- WCS User
- Guest User
- Operation
- Status
- Reason

Mesh Reports

- Alternate Parent
- Link Stats
- Nodes

- Packet Stats
- Stranded APss
- 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's capability to handle failures in the mesh path.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, 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 17-2 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 17-2 for more information on customizing report results.

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

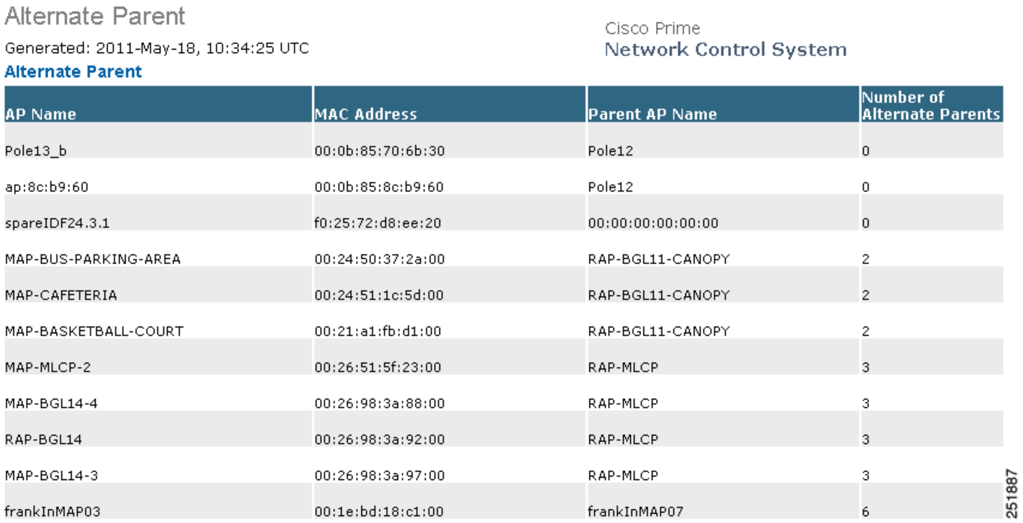
Available information for Alternate Parent report results includes:

- AP Name—The access point name.
- MAC address
- Parent AP name
- Number Alternate parents
- Parent MAC address

Alternate Parent Report Results

The Alternate Parent report contains the following results (Figure 17-27):

Figure 17-27 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.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Link Stats** or **Node Hops** from the drop-down list.
- Report by—Select **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 select 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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

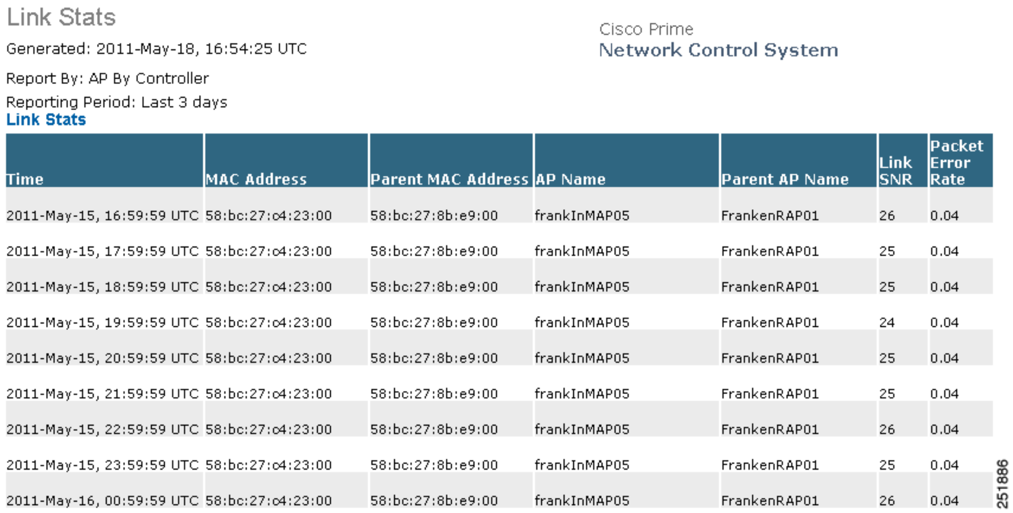
Available information for Link Stats report results includes:

- 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 Link Stats report contains the following results (Figure 17-28):

Figure 17-28 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

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.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, 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 17-2 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 17-2 for more information on customizing report results.

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

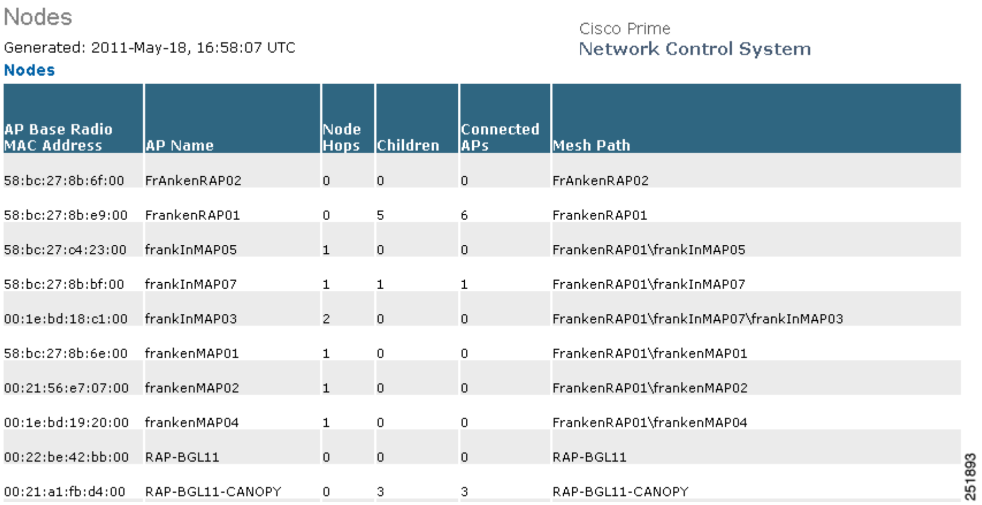
Available information for Node report results includes:

- 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 Node report contains the following results (Figure 17-29):

Figure 17-29 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

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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report Type—Select **Packet Stats** from the drop-down list.

- Report by—Select **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 select 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—Select 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. Select 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.

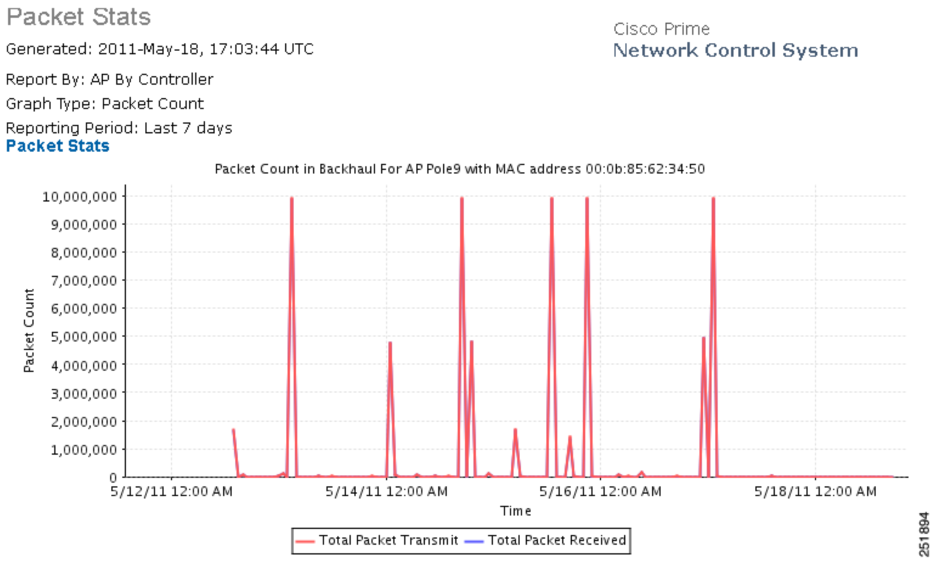
Schedule

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 17-2 for more information on scheduling a report.

Packet Stats Report Results

The Packet Stats report contains the following results (Figure 17-30):

Figure 17-30 Packet Stats Report Results



Packet Stats

Generated: 2011-May-18, 17:03:44 UTC

Report By: AP By Controller

Graph Type: Packet Count

Reporting Period: Last 7 days

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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report Type—Select **Packet Error Stats** from the drop-down list.
- Report by—Select **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 select 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—Select 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. Select 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.

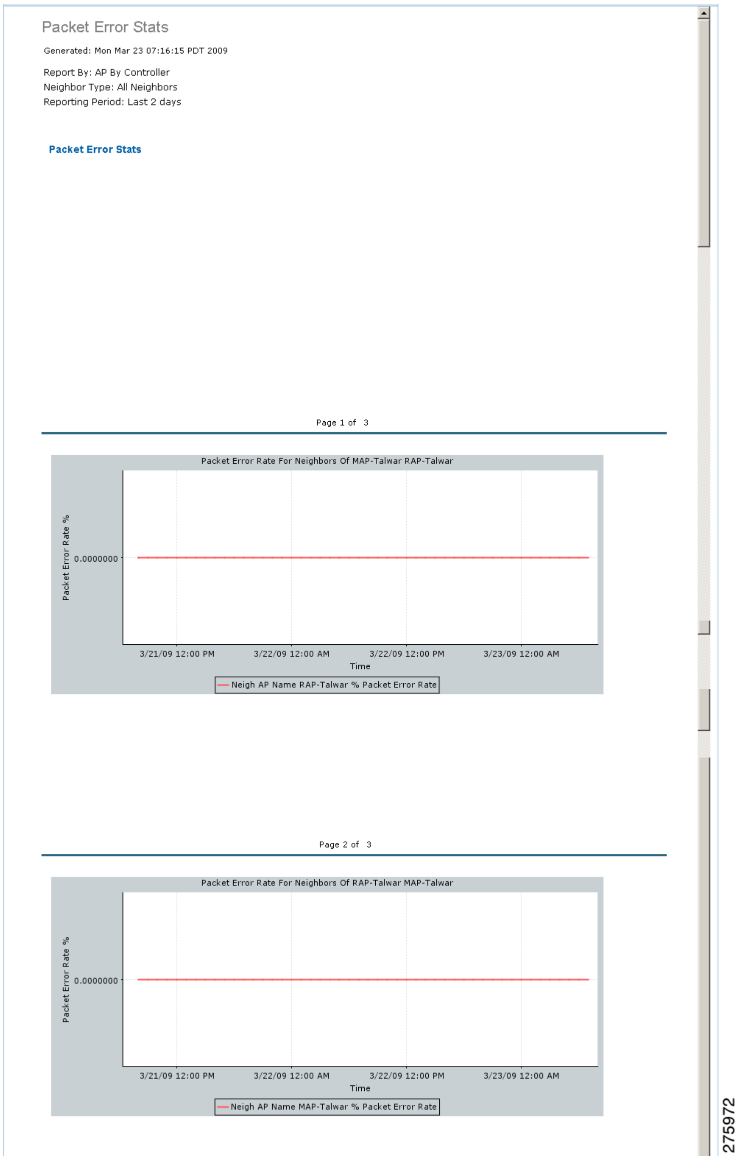
Schedule

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 17-2 for more information on scheduling a report.

Packet Error Stats Report Results

The Packet Error Statistics report contains the following results (Figure 17-31):

Figure 17-31 Packet Error Stats Report Results



Packet Error Stats

Generated: Mon Mar 23 07:16:15 PDT 2009

Report By: AP By Controller
Neighbor Type: All Neighbors
Reporting Period: Last 2 days

Packet Error Stats

Page 1 of 3

Packet Error Rate For Neighbors Of MAP-Talwar RAP-Talwar
Packet Error Rate %
0.0000000
3/21/09 12:00 PM
3/22/09 12:00 AM
3/22/09 12:00 PM
3/23/09 12:00 AM
Time
Neigh AP Name RAP-Talwar % Packet Error Rate

Page 2 of 3

Packet Error Rate For Neighbors Of RAP-Talwar MAP-Talwar
Packet Error Rate %
0.0000000
3/21/09 12:00 PM
3/22/09 12:00 AM
3/22/09 12:00 PM
3/23/09 12:00 AM
Time
Neigh AP Name MAP-Talwar % Packet Error Rate
275972

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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Packet Queue Stats** from the drop-down list.

- Report by—Select **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 select 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—Select the type of graph you want displayed for these report results (Packet Queue Average, Packets Dropped Count, 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. Select 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.

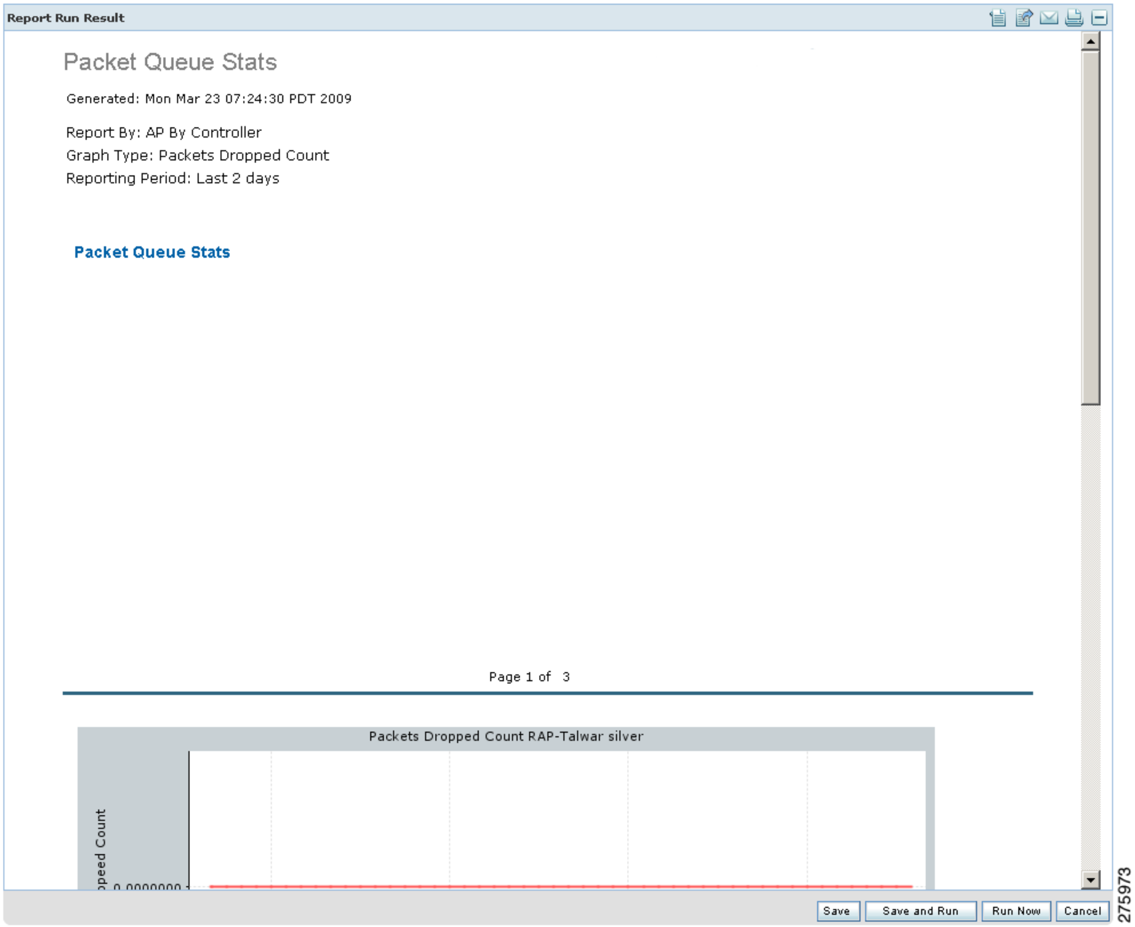
Schedule

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 17-2 for more information on scheduling a report.

Packet Queue Statistics Report Results

The Packet Queue Statistics report contains the following results (Figure 17-32):

Figure 17-32 Packet Queue Statistics Report Results



Report Run Result

Packet Queue Stats

Generated: Mon Mar 23 07:24:30 PDT 2009

Report By: AP By Controller
Graph Type: Packets Dropped Count
Reporting Period: Last 2 days

Packet Queue Stats

Page 1 of 3

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 WCS, or they might have never joined a controller managed by WCS.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Stranded States—Select **APs Managed by WCS** 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 17-2 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 17-2 for more information on customizing report results.

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

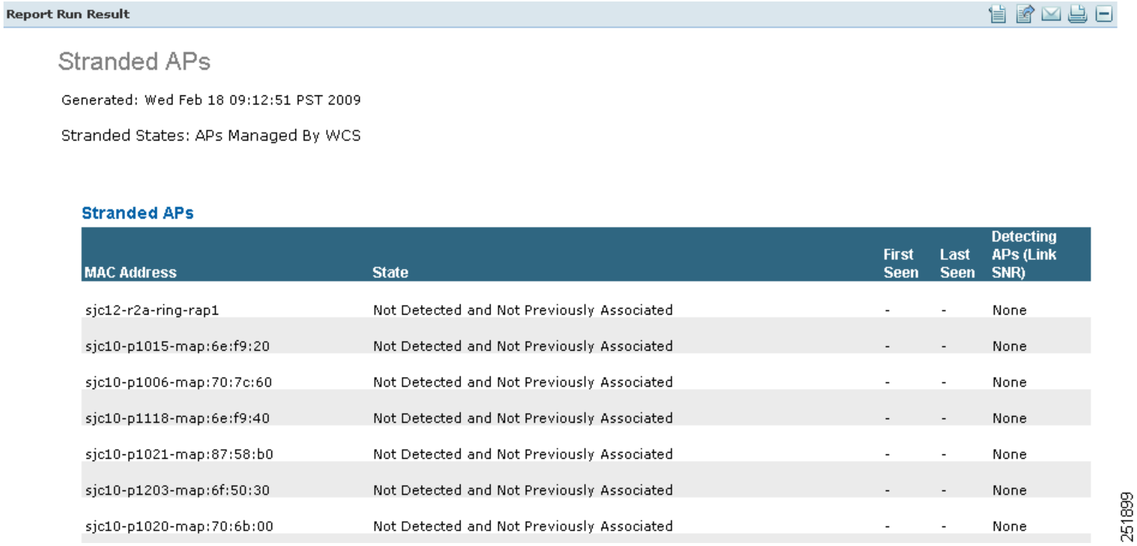
Available information for Link Stats report results includes:

- 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 Stranded APs report contains the following results (Figure 17-33):

Figure 17-33 Stranded APs Report Results



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

Worst Node Hops

This report displays the worst node hops or backhaul SNR links for the specified reporting period. The information displays 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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Worst Node Hops** or **Worst SNR Links** from the drop-down list.
- Report Type—When **Worst Node Hops** is selected from the Report Type above, select **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, select **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. Select 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 on each page.

  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 17-2 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 17-2 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, select the applicable section from the Customizable Report drop-down list.

Available information for Worst Node Hops report results includes:

- 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.

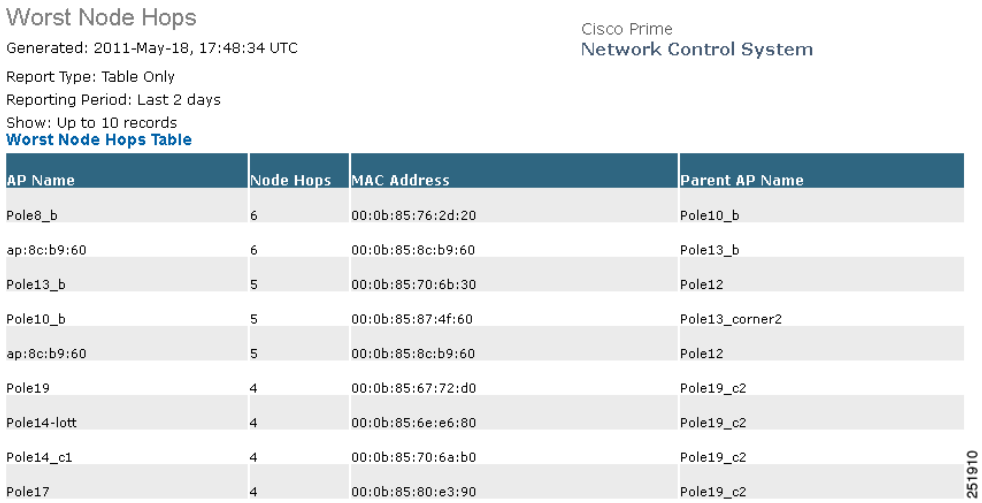
Available information for Worst SNR Links report results includes:

- 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 Worst Node Hops report contains the following results (Figure 17-34):

Figure 17-34 Worst Node Hops Report Results



Worst Node Hops

Generated: 2011-May-18, 17:48:34 UTC

Report Type: Table Only

Reporting Period: Last 2 days

Show: Up to 10 records

Worst Node Hops Table

AP Name	Node Hops	MAC Address	Parent AP Name
Pole8_b	6	00:0b:85:76:2d:20	Pole10_b
ap:8c:b9:60	6	00:0b:85:8c:b9:60	Pole13_b
Pole13_b	5	00:0b:85:70:6b:30	Pole12
Pole10_b	5	00:0b:85:87:4f:60	Pole13_corner2
ap:8c:b9:60	5	00:0b:85:8c:b9:60	Pole12
Pole19	4	00:0b:85:67:72:d0	Pole19_c2
Pole14-lott	4	00:0b:85:6e:e6:80	Pole19_c2
Pole14_c1	4	00:0b:85:70:6a:b0	Pole19_c2
Pole17	4	00:0b:85:80:e3:90	Pole19_c2

Network Summary

- 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.

This report contains the following settings and scheduling parameters:

Settings

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

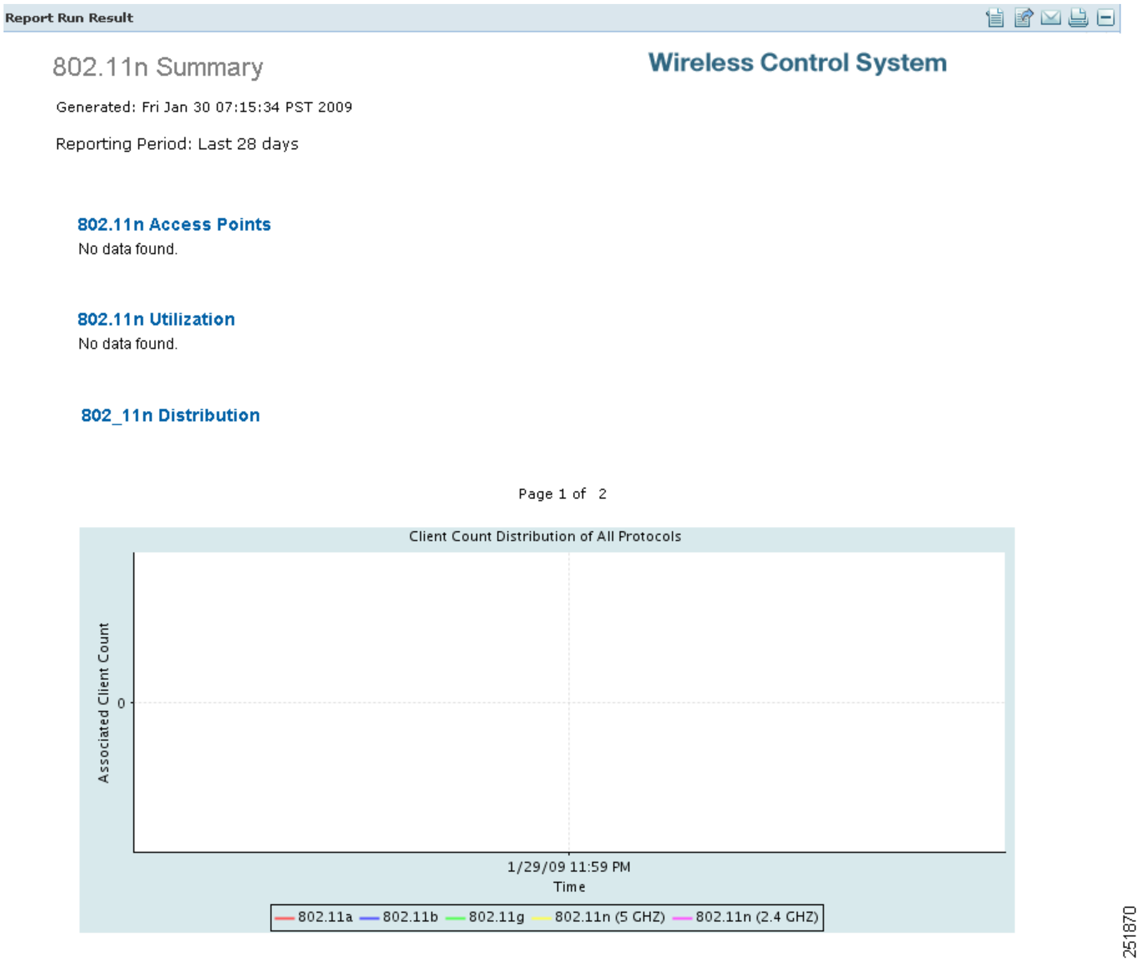
Schedule

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 17-2 for more information on scheduling a report.

802.11n Summary Report Results

The 802.11n Summary report contains the following results (Figure 17-35):

Figure 17-35 802.11n Summary Report Results



802.11n Summary

Generated: Fri Jan 30 07:15:34 PST 2009

Reporting Period: Last 28 days

802.11n Access Points

No data found.

802.11n Utilization

No data found.

802_11n Distribution

Executive Summary

This report displays a quick view of your wireless network. It provides details on LWAPP versus autonomous access point usage, associated client counts in the network, and guest client counts in the network.

This report contains the following settings and scheduling parameters:

Settings

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

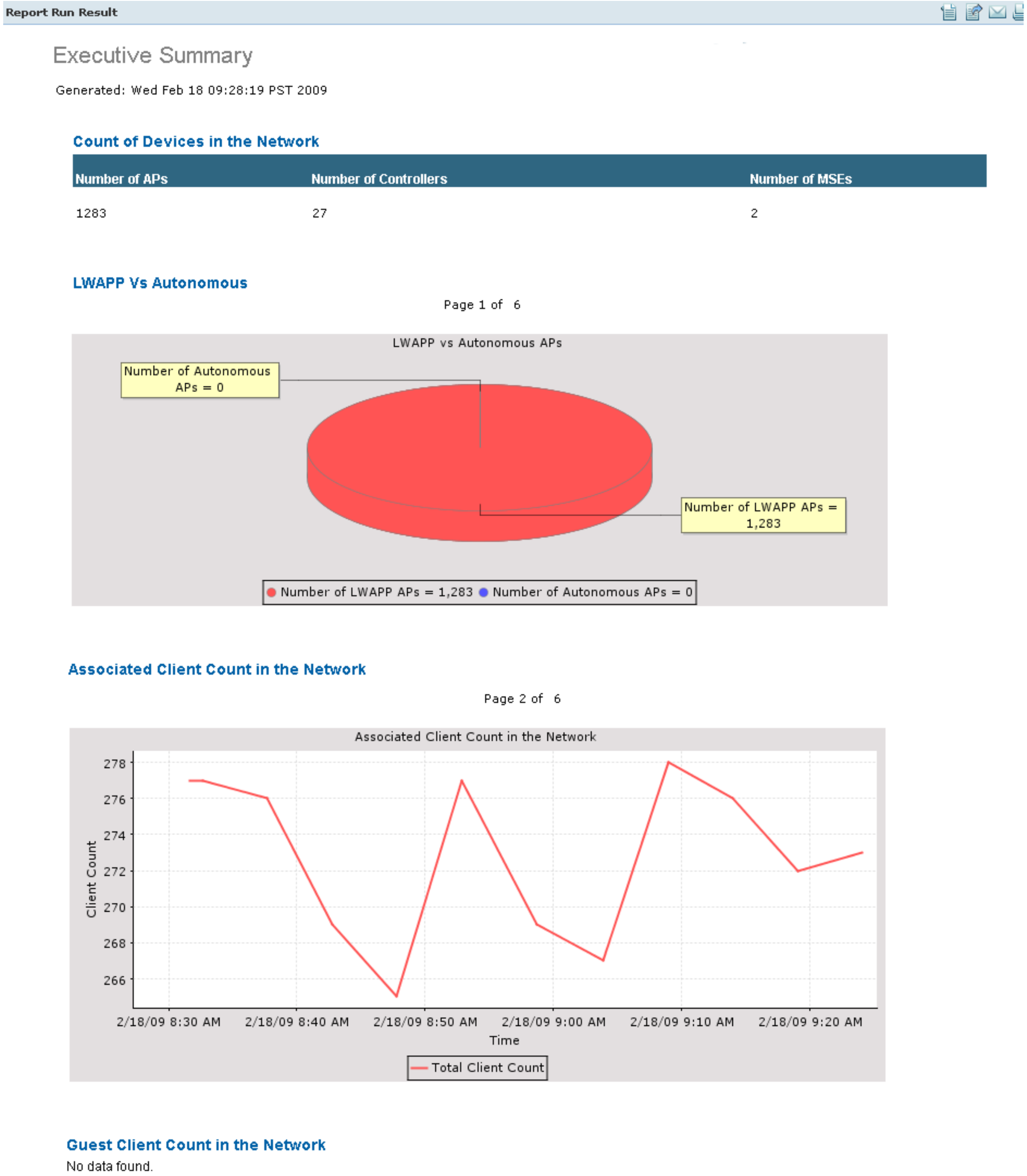
Schedule

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 17-2 for more information on scheduling a report.

Executive Summary Report Results

The Executive Summary report results contain the following (Figure 17-36):

Figure 17-36 Executive Summary Report Results



Report Run Result

Executive Summary

Generated: Wed Feb 18 09:28:19 PST 2009

Count of Devices in the Network

Number of APs	Number of Controllers	Number of MSEs
1283	27	2

LWAPP Vs Autonomous

Page 1 of 6

LWAPP vs Autonomous APs
Number of Autonomous APs = 0
Number of LWAPP APs = 1,283
● Number of LWAPP APs = 1,283 ● Number of Autonomous APs = 0

Associated Client Count in the Network

Page 2 of 6

Guest Client Count in the Network

No data found.

Performance Reports

You can create 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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select 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—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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

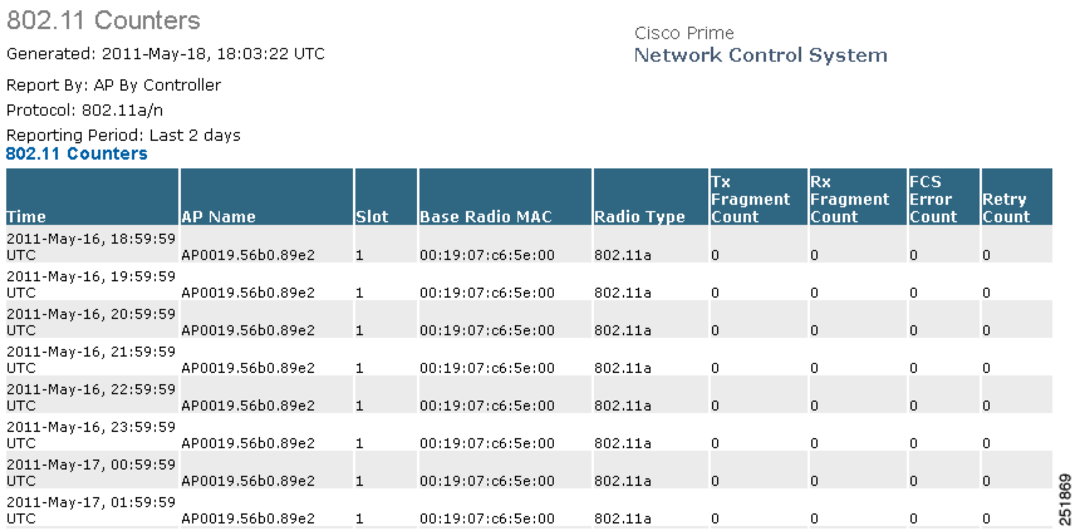
Available information for 802.11 Counters report results includes:

- 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 AT's 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.

802.11 Counters Report Results

The 802.11 Counter report contains the following results (Figure 17-37):

Figure 17-37 802.11 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

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 decide whether you need additional access points to provide coverage in sparsely deployed areas. It runs on the alarm table and both the alarm generation time, the cleared time (if cleared), and the state of the alarm (active or cleared).

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select 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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

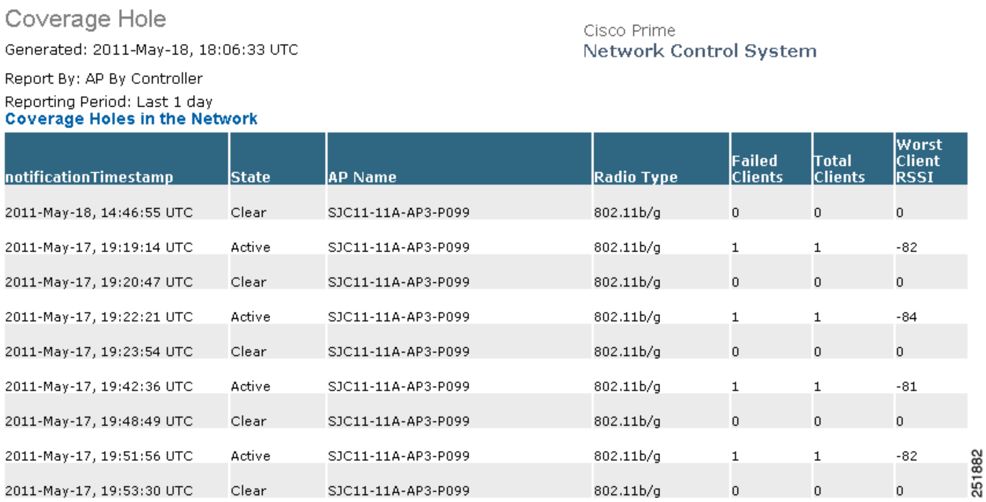
Available information for Coverage Hole report results includes:

- 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 Coverage Hole report contains the following results (Figure 17-38):

Figure 17-38 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 use based on the aggregated port use of all controllers on your network. With these statistics, you can assess current network performance and plan for future scalability needs.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, 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. Select 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 17-2 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 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available data fields column.

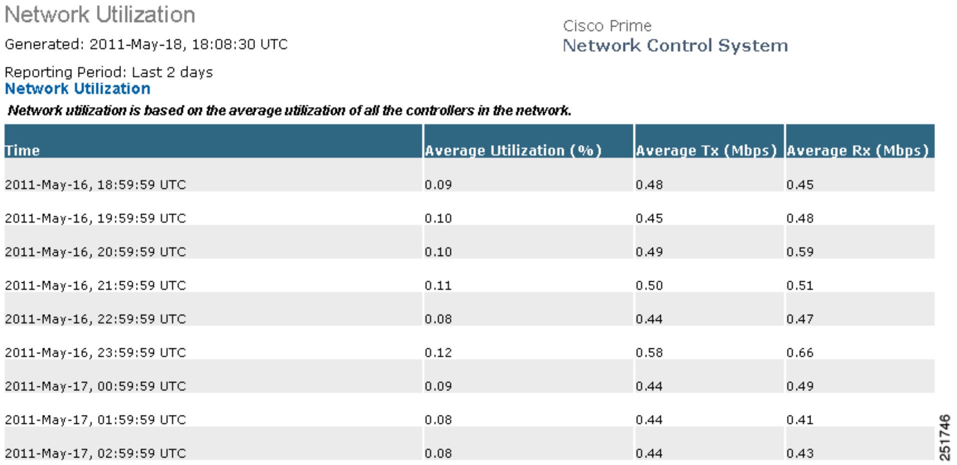
Available information for the Network Utilization report results includes:

- Time
- Average Utilization (%)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.
- Average Tx (Mbps)—The average aggregated received Mbs of all ports on all controllers.
- Average Rx (Mbps)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.

Network Utilization Report Results

The Network Utilization report contains the following results (Figure 17-39):

Figure 17-39 Network Utilization Report Results



Network Utilization

Generated: 2011-May-18, 18:08:30 UTC

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

Traffic Stream Metrics

This report can help you identify 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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select 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—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. Select 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 17-2 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 17-2 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 includes:

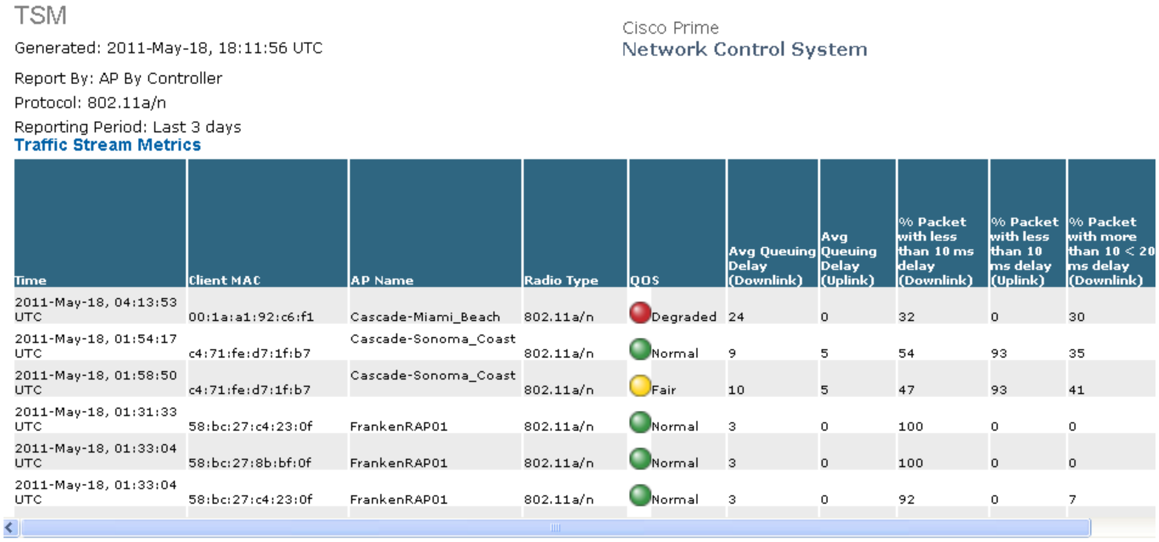
- Time—Date and time the statistics were recorded.
- MAC address—The MAC address of the access point.
- AP Name—The access point name.
- Radio Type—802.11a/n or 802.11b/g/n.
- Average Queuing Delay (Downlink)—The average queuing delay for downlinks.
- Average Queuing Delay (Uplink)—The average queuing 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 Traffic Stream Metrics report contains the following results (Figure 17-40):

Figure 17-40 Traffic Stream Metrics Report Results



TSM

Generated: 2011-May-18, 18:11:56 UTC

Cisco Prime
Network Control System

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

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)
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
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
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
2011-May-18, 01:31:33 UTC	58:bc:27:c4:23:0f	FrankenRAP01	802.11a/n	● Normal	3	0	100	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
2011-May-18, 01:33:04 UTC	58:bc:27:c4:23:0f	FrankenRAP01	802.11a/n	● Normal	3	0	92	0	7

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 could help identify unexpected behavior or network performance problems.

This report contains the following settings and scheduling parameters:

Settings

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

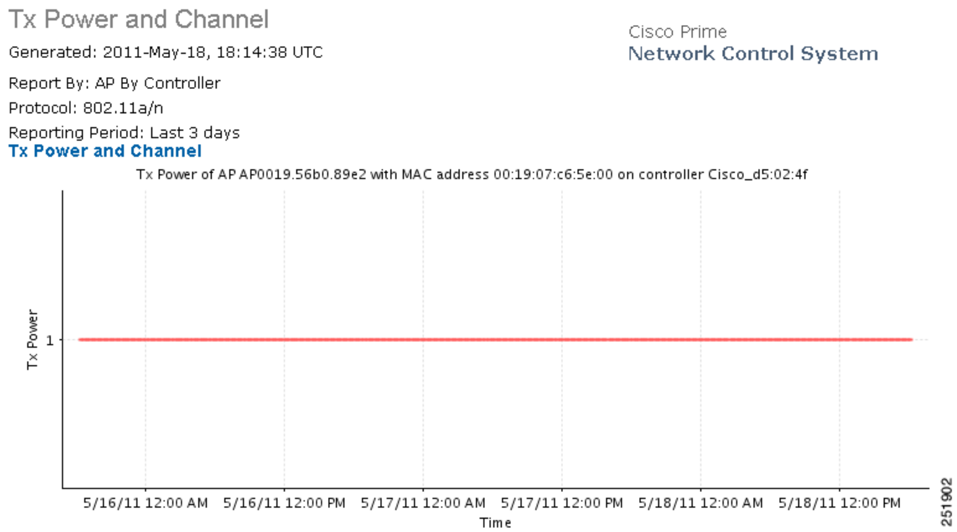
Schedule

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 17-2 for more information on scheduling a report.

Tx Power and Channel Report Results

The Tx Power and Channel report contains the following results (Figure 17-41):

Figure 17-41 Tx Power and Channel Report Results



Tx Power and Channel

Generated: 2011-May-18, 18:14:38 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

VoIP Calls Graph

This report helps you 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, you must enable Media Session Snooping on the WLAN. This report displays information in a graph.

Note MSA only supports SIP calls.

This report contains the following settings and scheduling parameters:

Settings

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

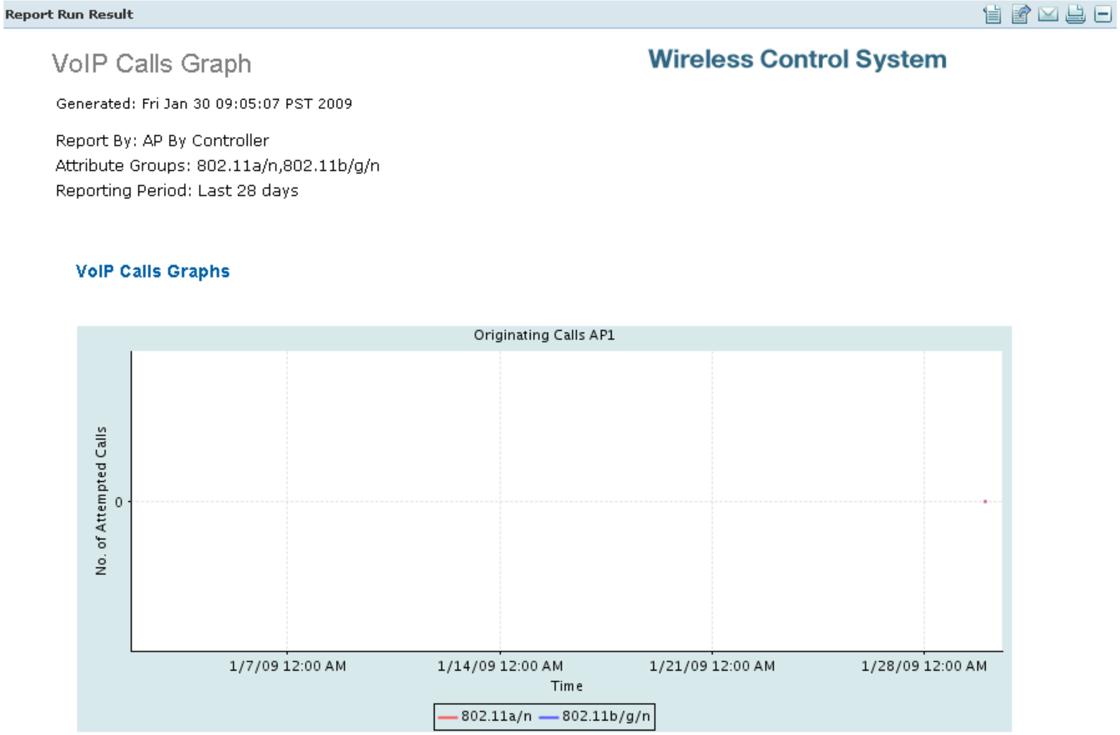
Schedule

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 17-2 for more information on scheduling a report.

VoIP Calls Report Results

The VoIP Calls report contains the following results (Figure 17-42):

Figure 17-42 VoIP Calls Graph Results



Report Run Result

VoIP Calls Graph

Wireless Control System

Generated: Fri Jan 30 09:05:07 PST 2009

Report By: AP By Controller
Attribute Groups: 802.11a/n,802.11b/g/n
Reporting Period: Last 28 days

VoIP Calls Graphs

251908

VoIP Calls Table

This report helps you 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, you must enable VoIP snooping (also called Media Session Aware or MSA) on the WLAN. This report displays information in a table.

This report contains the following settings and scheduling parameters:

Settings

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

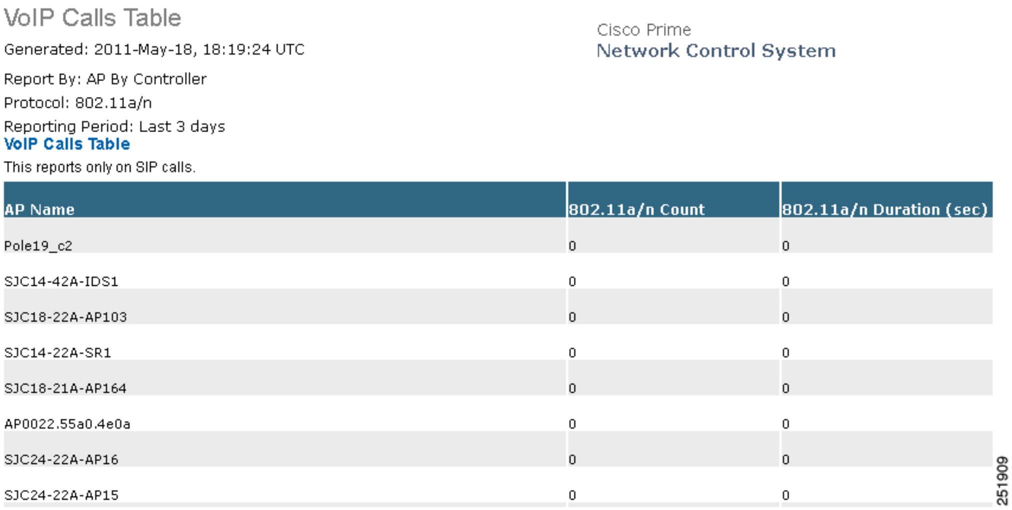
Schedule

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 17-2 for more information on scheduling a report.

VoIP Calls Table Results

The VoIP Table report contains the following results (Figure 17-43):

Figure 17-43 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

Cisco Prime
Network Control System

VoIP Calls Table

This reports only on SIP calls.

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

Voice Statistics

This report helps you analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, non-roaming calls, and rejected calls (per radio) on the network. To gather useful data from this report, you must make sure that call admission control (CAC) is supported on voice clients.

This report contains the following settings and scheduling parameters:

Settings

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

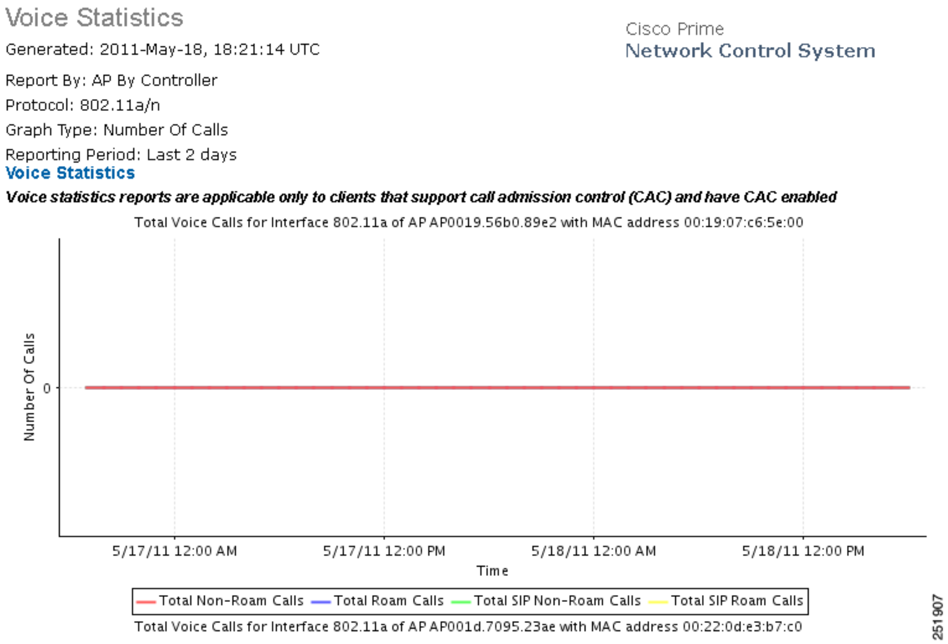
Schedule

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 17-2 for more information on scheduling a report.

Voice Statistics Results

The Voice Statistics report contains the following results (Figure 17-44):

Figure 17-44 Voice Statistics Results



Voice Statistics

Generated: 2011-May-18, 18:21:14 UTC

Report By: AP By Controller
Protocol: 802.11a/n
Graph Type: Number Of Calls
Reporting Period: Last 2 days

Cisco Prime
Network Control System

Voice Statistics

Voice statistics reports are applicable only to clients that support call admission control (CAC) and have CAC enabled

Total Voice Calls for Interface 802.11a of AP AP0019.56b0.89e2 with MAC address 00:19:07:c6:5e:00

Total Voice Calls for Interface 802.11a of AP AP001d.7095.23ae with MAC address 00:22:0d:e3:b7:c0

Security Reports

You can create the following security reports:

- Adaptive wIPS Alarms
- Adaptive wIPS Top 10 Access Points
- Adhoc Rogue Events
- Adhoc Rogues
- New Rogue Access Points
- New Rogue Access Point Count
- Rogue Access Points Events
- Rogue Access Points
- Security Summary

Adaptive wIPS Alarms

This report displays wIPS events by selected MSEs, controllers, and access points for each alarm type. This report can take awhile to generate if you set the reporting criteria to collect a substantial number of events. It is best to give a short duration time or run it as a scheduled report.

This report contains thee following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - MSE with Adaptive wIPS Service—Select **All MSEs with Adaptive wIPS Service** from the Report Criteria page or click **Edit** to select a specific MSE.
  - Controller by MSE—Select **All MSEs > All Controllers** from the Report Criteria page or click **Edit** to select a specific controller.
  - AP by MSE—Select **All MSEs > All Controllers > All APs** from the Report Criteria page or click **Edit** to select a specific access point.

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

- Alarm Category—Select **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the 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. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are shown in WCS server local time.

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 17-2 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 17-2 for more information on customizing report results.

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

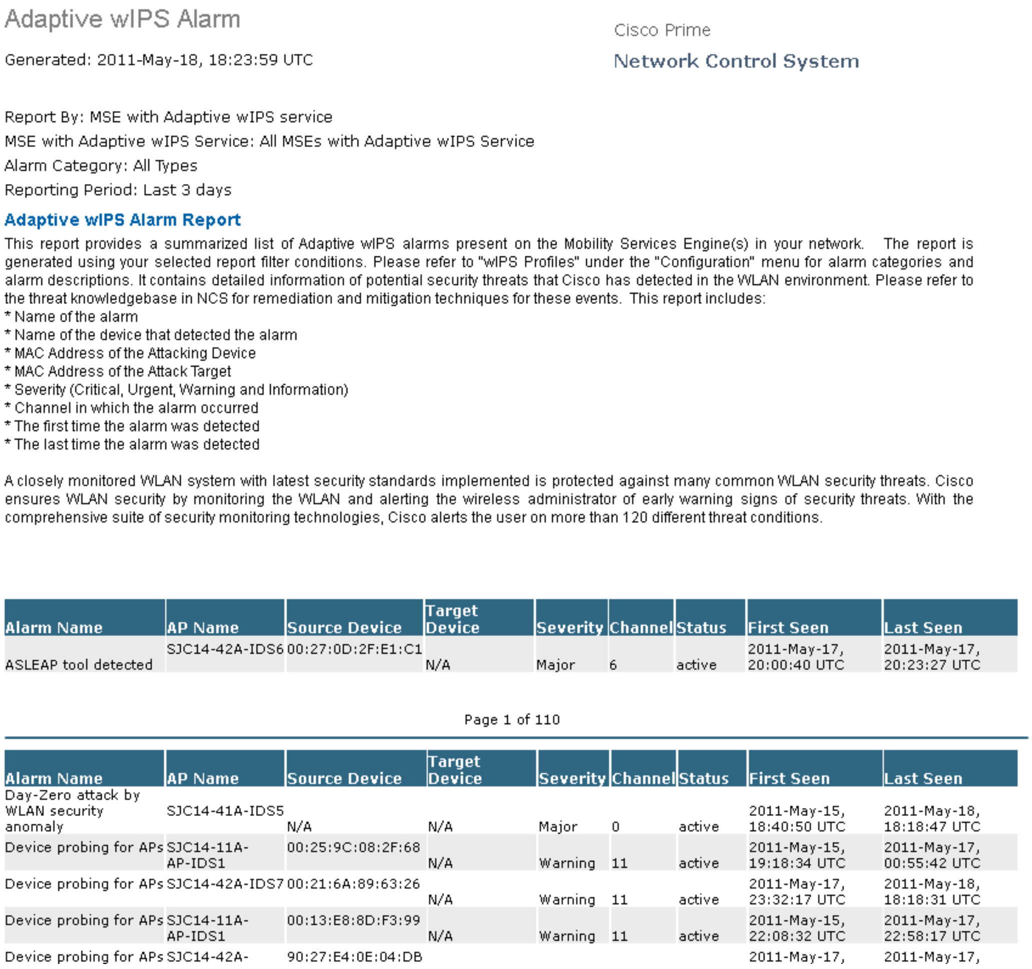
The following information is available for an Adaptive wIPS Alarms report:

- Alarm Name—The name of the alarm.
- 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—The type of alarm.
- MSE Name—The name of the MSE to which this device is associated.

Adaptive wIPS Alarms Report Results

The Adaptive wIPS Alarms report contains the following results (Figure 17-45):

Figure 17-45 Adaptive wIPS Alarms Report



Adaptive wIPS Alarm

Generated: 2011-May-18, 18:23:59 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 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,

Adaptive wIPS Top 10 Access Points

This report displays the ten access points with the highest number of generated Adaptive wIPS alarms.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - MSE with Adaptive wIPS Service—Select **All MSEs with Adaptive wIPS Service** from the Report Criteria page or click **Edit** to select a specific MSE.
  - Controller by MSE—Select **All MSEs > All Controllers** from the Report Criteria page or click **Edit** to select a specific controller.

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

- Alarm Category—Select **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
  - 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. Select the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time.

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 17-2 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 17-2 for more information on customizing report results.

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

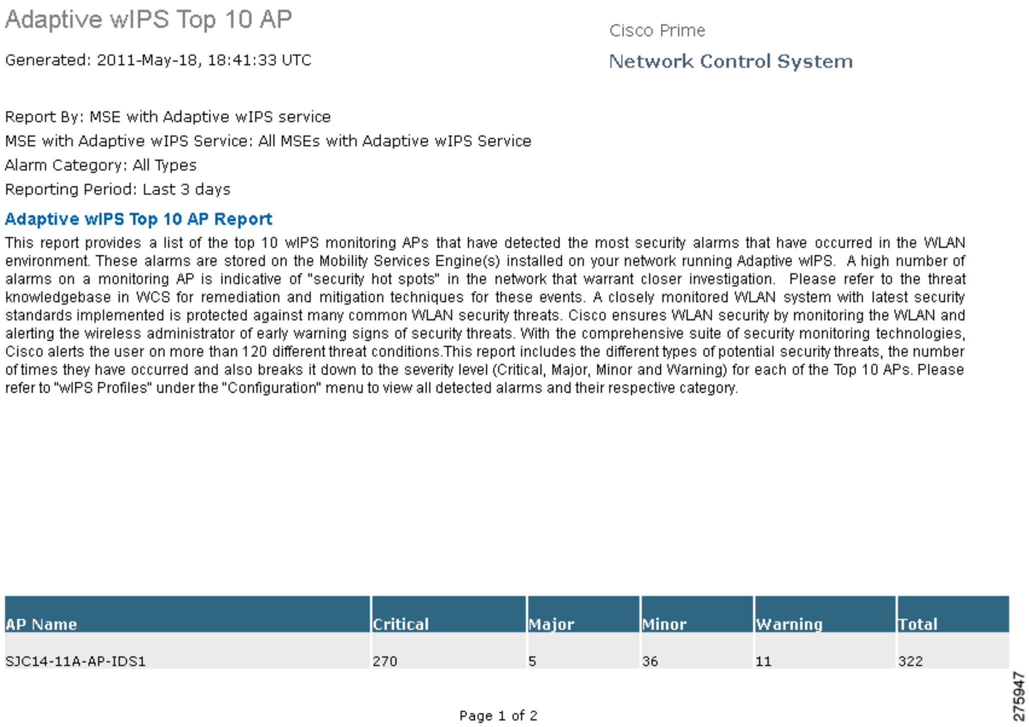
The following information is available for an Adaptive wIPS Top 10 Access Points report:

- AP Name—The name of the access point that generated the alarm.
- 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.

Adaptive wIPS Top 10 Access Points Report Results

The following is an example of an Adaptive wIPS Top 10 Access Points report (Figure 17-46):

Figure 17-46 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

Adhoc Rogue Events

This report displays all ad hoc rogue events received by WCS.

This report contains the following settings and scheduling parameters:

Settings

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

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 17-2 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 17-2 for more information on customizing report results.

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

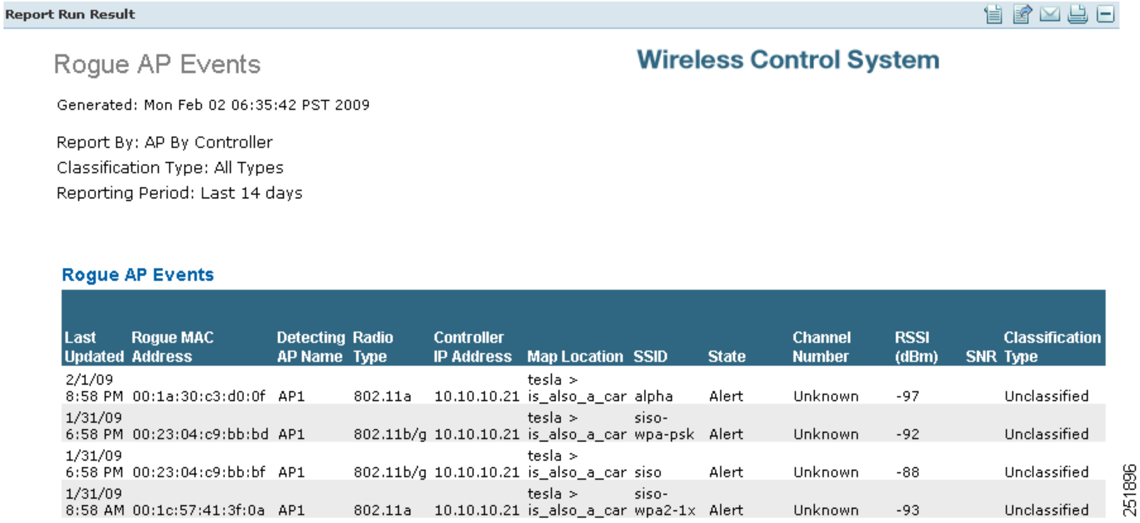
The following information is available for an Adhoc Rogue Events report:

- Last Seen Time—Date and time the ad hoc rogue was last seen.
- Rogue MAC Address—The MAC address of the rogue access point.
- Detecting AP Name—The name of the access point that detected the rogue.
- Radio Type—802.11a or 802.11b/g.
- 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.
- Channel Number—The channel number of the ad hoc rogue.
- RSSI (dBm)—The received signal strength indicator in dBm.

Adhoc Rogue Events Report Results

The Adhoc Rogue Events report contains the following results (Figure 17-47):

Figure 17-47 Adhoc Rogue Events Results



Report Run Result

Rogue AP Events

Wireless Control System

Generated: Mon Feb 02 06:35:42 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 14 days

Rogue AP Events

Last Updated	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	State	Channel Number	RSSI (dBm)	SNR	Classification Type
2/1/09 8:58 PM	00:1a:30:c3:d0:0f	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	alpha	Alert	Unknown	-97		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bd	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso-wpa-psk	Alert	Unknown	-92		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bf	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso	Alert	Unknown	-88		Unclassified
1/31/09 8:58 AM	00:1c:57:41:3f:0a	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	siso-wpa2-1x	Alert	Unknown	-93		Unclassified

Adhoc Rogues

WCS gets updates about ad hoc rogues from the controller by using traps or polling. The Last Seen Time is updated anytime a trap for the ad hoc rogue is received or the ad hoc rogue was seen during the last polling cycle of WCS. This report is based on the last seen time of the ad hoc rogue. It includes those rogue access point alarms with clear severity.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select 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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

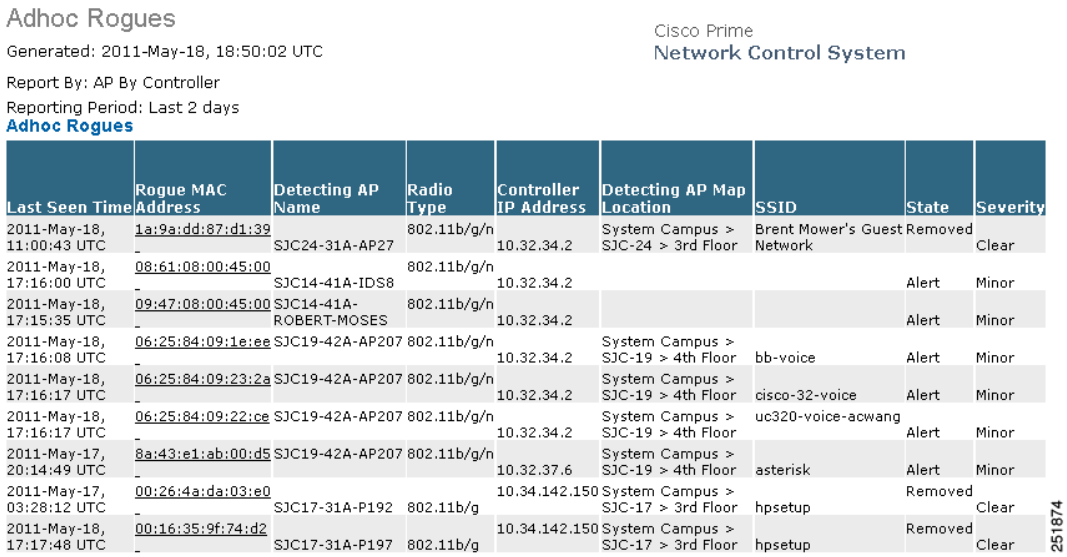
The following information is available for an Adhoc Rogues report:

- 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.

Adhoc Rogues Report Results

The Adhoc Rogues report contains the following results (Figure 17-48):

Figure 17-48 Adhoc Rogues Results



Adhoc Rogues

Generated: 2011-May-18, 18:50:02 UTC

Report By: AP By Controller

Reporting Period: Last 2 days

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

New Rogue Access Points

This report displays all new rogues detected for the first time within a selected timeframe on your network. This report is based on the first seen time of the rogue and is sorted as such. The report includes those rogue access point alarms with clear severity. The value in the Created Time column indicates the time the rogue was first detected.

This report contains the following settings and scheduling parameters:

Settings

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

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

- Classification Type—Select **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. Select 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 "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

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

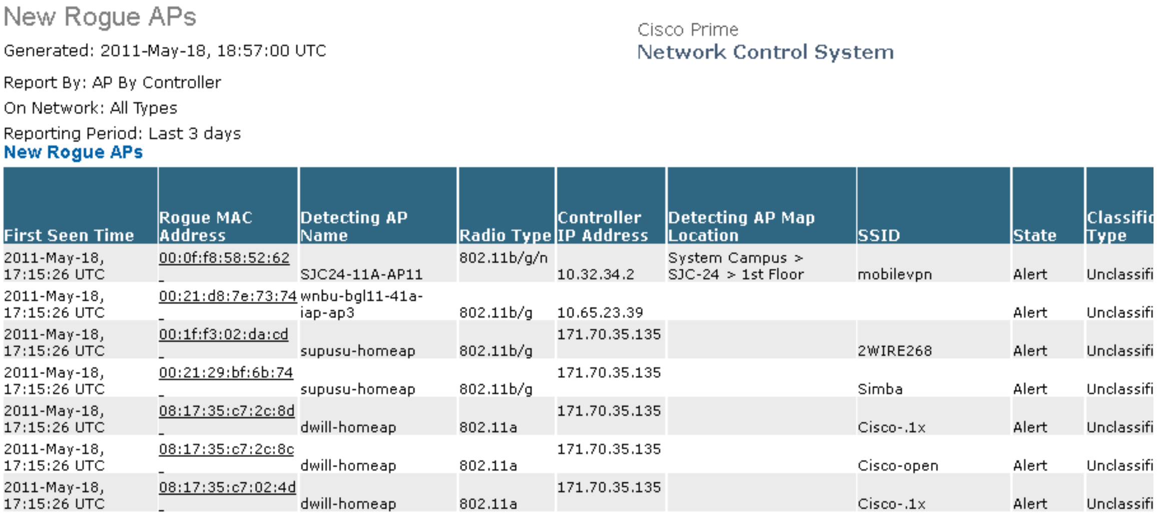
The following information is available for a New Rogue Access Points report:

- 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.
- 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.

New Rogue APs Report Results

The New Rogue Access Points report contains the following results (Figure 17-49):

Figure 17-49 New Rogue Access Points Report



New Rogue APs

Generated: 2011-May-18, 18:57:00 UTC

Cisco Prime
Network Control System

Report By: AP By Controller

On Network: All Types

Reporting Period: Last 3 days

New Rogue APs

First Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Classific Type
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	Unclassifi
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	Unclassifi
2011-May-18, 17:15:26 UTC	00:1f:f3:02:da:cd	supusu-homeap	802.11b/g	171.70.35.135		2WIRE268	Alert	Unclassifi
2011-May-18, 17:15:26 UTC	00:21:29:bf:6b:74	supusu-homeap	802.11b/g	171.70.35.135		Simba	Alert	Unclassifi
2011-May-18, 17:15:26 UTC	08:17:35:c7:2c:8d	dwill-homeap	802.11a	171.70.35.135		Cisco-.1x	Alert	Unclassifi
2011-May-18, 17:15:26 UTC	08:17:35:c7:2c:8c	dwill-homeap	802.11a	171.70.35.135		Cisco-open	Alert	Unclassifi
2011-May-18, 17:15:26 UTC	08:17:35:c7:02:4d	dwill-homeap	802.11a	171.70.35.135		Cisco-.1x	Alert	Unclassifi

New Rogue Access Point Count

This report provides a graphical display of the count of new rogue access points detected for the first time within the specified time interval. The report includes those rogue access point alarms with clear severity.

This report contains the following settings and scheduling parameters:

Settings

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

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

- Classification Type—Select **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. Select 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.

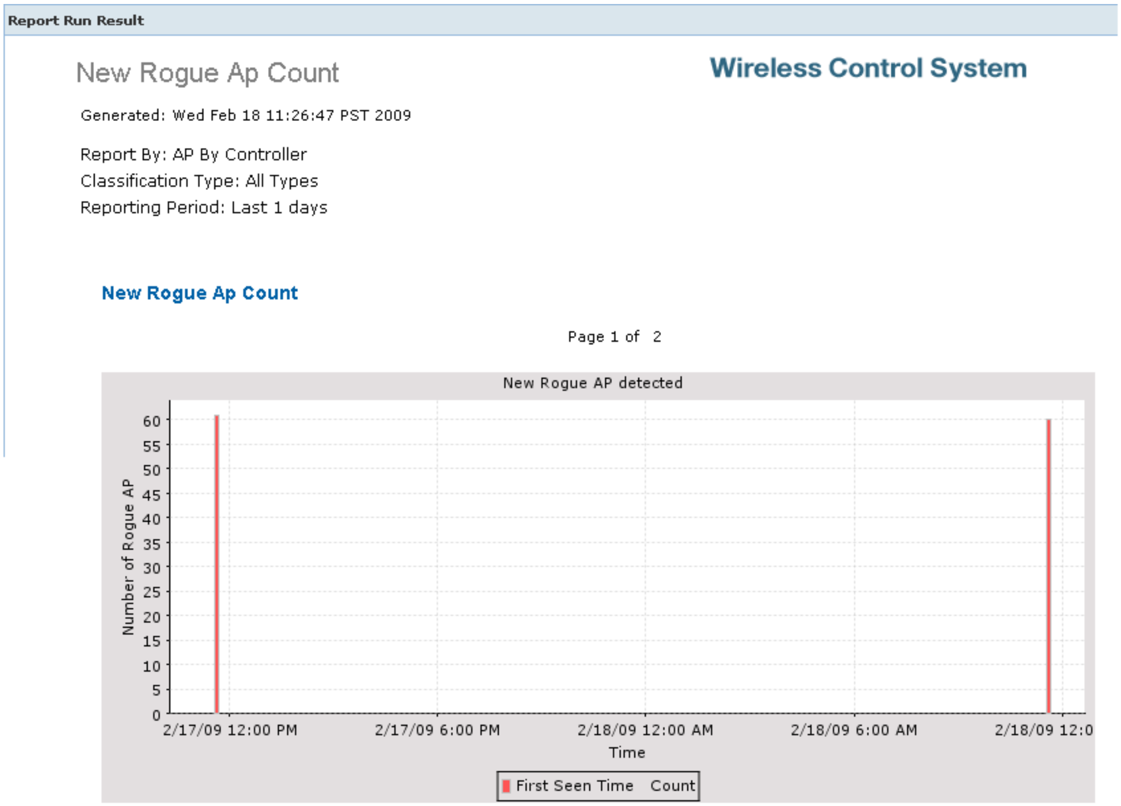
Schedule

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 17-2 for more information on scheduling a report.

New Rogue Access Point Count Report Results

The New Rogue Access Point Count report contains the following results (Figure 17-50):

Figure 17-50 New Rogue Access Point Count Report



Report Run Result

New Rogue Ap Count

Wireless Control System

Generated: Wed Feb 18 11:26:47 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 1 days

New Rogue Ap Count

Page 1 of 2

251890

Rogue Access Points Events

This report displays all rogue access point events received by WCS based on the event time of the rogue access points. Any rogue-related trap received by WCS is logged as a rogue event in WCS. A new rogue access point event is created by WCS based on polled data when there is a newly detected rogue access point. In addition, an event is also created by WCS when the user changes the state and classification of the rogue access point through the WCS user interface. One rogue can have multiple events. This report is sorted based on the timestamp of the event.

This report contains the following settings and scheduling parameters:

Settings

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

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

- Classification Type—Select **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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

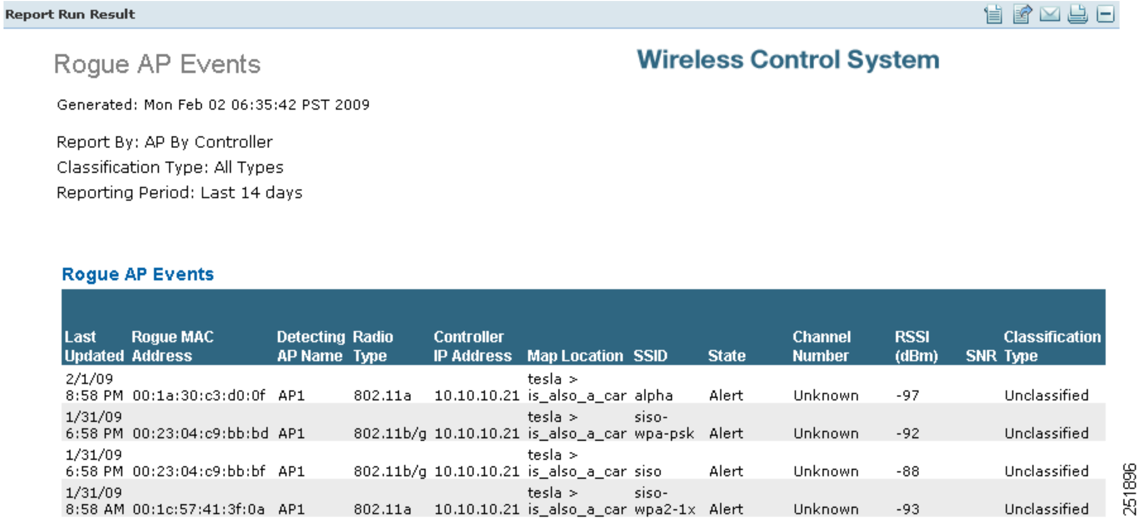
The following information is available for a Rogue Access Point Events report:

- 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.
- 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/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 maximum received signal strength indicator ever reported by any controller for this rogue.
- SNR—The Signal-to-Noise Ratio.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).

Rogue AP Events Report Results

The Rogue Access Point Events report contains the following results (Figure 17-51):

Figure 17-51 Rogue Access Point Events Report



Rogue AP Events

Generated: Mon Feb 02 06:35:42 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 14 days

Rogue AP Events

Last Updated	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	State	Channel Number	RSSI (dBm)	SNR	Classification Type
2/1/09 8:58 PM	00:1a:30:c3:d0:0f	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	alpha	Alert	Unknown	-97		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bd	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso-wpa-psk	Alert	Unknown	-92		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bf	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso	Alert	Unknown	-88		Unclassified
1/31/09 8:58 AM	00:1c:57:41:3f:0a	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	siso-wpa2-1x	Alert	Unknown	-93		Unclassified

Rogue Access Points

WCS gets updates about rogues from controllers using traps or polling. The last seen time is updated whenever a trap for the rogue is received or rogue was detected during the last polling cycle of WCS. This report is based on the last seen time of the rogue access point. It includes those rogue access point alarms with clear severity.

This report contains the following settings and scheduling parameters:

Settings

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

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

- Classification Type—Select **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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

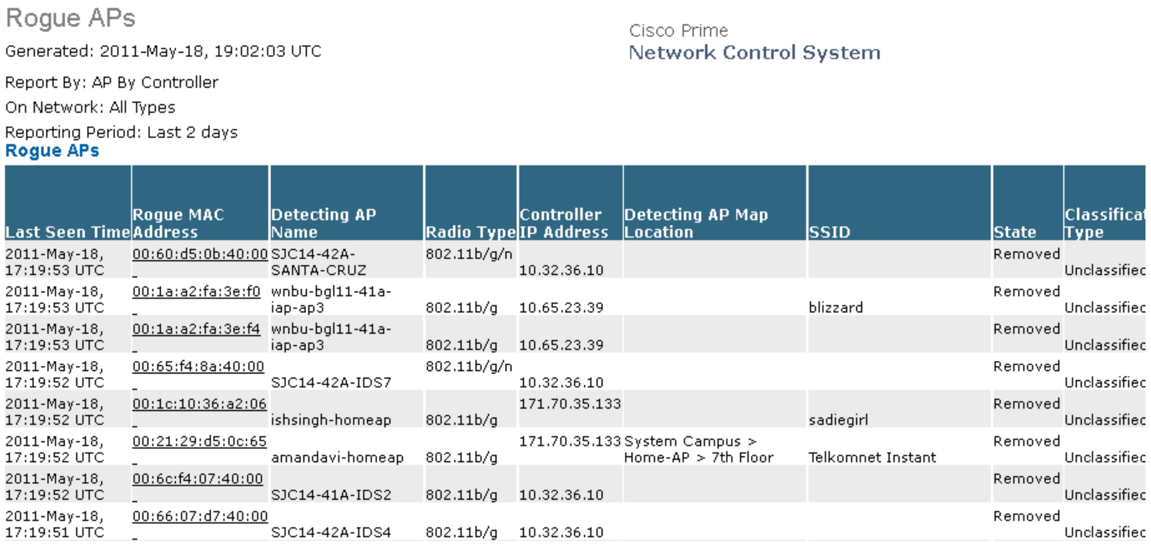
The following information is available for a Rogue APs report:

- 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.
- 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.

Rogue APs Report Results

The Rogue Access Points report contains the following results (Figure 17-52):

Figure 17-52 Rogues APs Report



Rogue APs

Generated: 2011-May-18, 19:02:03 UTC

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	Classificat Type
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	Unclassifiec
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	Unclassifiec
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	Unclassifiec
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	Unclassifiec
2011-May-18, 17:19:52 UTC	00:1c:10:36:a2:06	ishsingh-homeap	802.11b/g	171.70.35.133		sadiegirl	Removed	Unclassifiec
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	Unclassifiec
2011-May-18, 17:19:52 UTC	00:6c:f4:07:40:00	SJC14-41A-IDS2	802.11b/g	10.32.36.10			Removed	Unclassifiec
2011-May-18, 17:19:51 UTC	00:66:07:d7:40:00	SJC14-42A-IDS4	802.11b/g	10.32.36.10			Removed	Unclassifiec

Security Summary

This report displays the number of association failures, rogue access points, ad hocs, and access point connections or disconnections over one month.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, 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. Select 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 17-2 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 17-2 for more information on customizing report results.

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

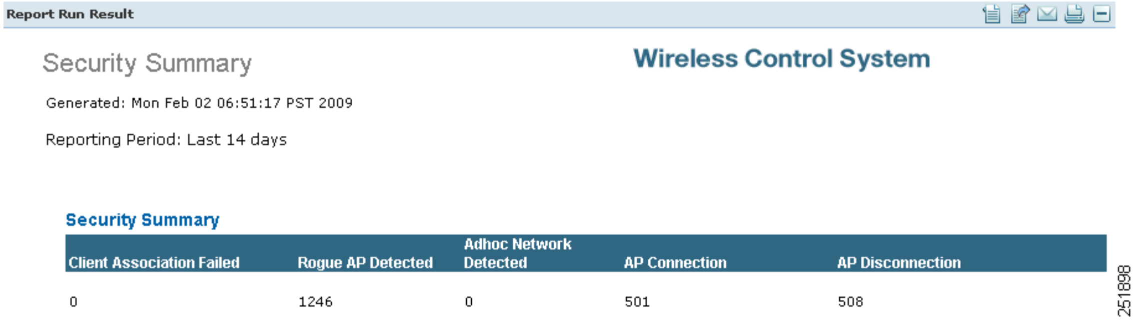
The following information is available for a Security Summary report:

- Client Association Failed—The number of client association failures during the specified period of time.
- Rogue AP Detected—The number of rogue access points detected during the specified period of time.
- Adhoc Network Detected—The number of ad hoc networks detected during the specified period of time.
- AP Connection—The number of access point connections during the specified period of time.
- AP Disconnection—The number of access point disconnections during the specified period of time.

Security Summary Report Results

The Security Summary report contains the following results (Figure 17-53):

Figure 17-53 Security Summary Report



Report Run Result

Security Summary

Generated: Mon Feb 02 06:51:17 PST 2009

Reporting Period: Last 14 days

Security Summary

Client Association Failed	Rogue AP Detected	Adhoc Network Detected	AP Connection	AP Disconnection
0	1246	0	501	508