CHAPTER 11

Using Reports

In Cisco netManager, reports are used to troubleshoot and monitor performance and historical data that has been collected during the operation of the application. These reports can help you troubleshoot problem areas on your network and give you easy access to important network information.

Report Categories

There are three categories for reports based on the scope of information displayed within a report:

- **System**—These reports display system-wide information. System reports do not focus on a particular device or a specific device group. Examples of system reports include the General Error Log and the Web User Activity Log.
- **Group**—These reports display information relating to a specific device group. Examples of group reports include the Group State Change Timeline and the Group Actions Applied reports.
- **Device**—These reports display information relating to a specific device. An example of a device report is the Device Status Report.

There are four categories for reports based on the type of information displayed within a report:

- **Performance**—These reports display information gathered from SNMP performance monitors regarding your network devices' CPU, disk, interface, and memory utilization, and ping latency and availability.

Note All performance monitors except interface utilization, and ping latency and availability are associated and selected by default. The default reports will be generated automatically. To begin collecting performance data for interface utilization, and ping latency and availability, right-click a device from the Devices tab and select **Properties** from the context menu. In the Device Properties dialog box, select **Performance Monitors**. Information will not be displayed in performance reports until you have done this.

- **Problem Areas**—These are troubleshooting reports that allow you to investigate network issues. Examples of problem area reports include the Group Active Monitor Outage and the Passive Monitor Error Log.
- **General**—These reports display information on your Cisco netManager settings and diagnostics, as well as device-specific and user-configured details. The Home, Top 10, and Device Status workspaces/ reports all fall in the General category.

- **Phone Reports**—These reports display information about the phone, such as extension, description, MAC address, IP address, and model. Examples of phone reports include IP Phone Audit and IP Phone Move.

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

Selecting a Report

From the Reports tab, you can use the Report Navigation Menu to view report indexes. From here you can choose to view indexes for:

- All reports
- All reports in a certain category (System, Group, Device)
- All reports of a certain type (Performance, Problem Areas, Inventory, General)
- Reports you have added as Favorites

After you have opened a report index, double-click the report you want to view.

To open the complete Report tree, click **GO > Report > All**. You can expand each report category and type by clicking the + button to view the reports within each section. Double-click a report to view it.

About Data Collection for Reports

Data for reports is collected by default as follows:

- The raw data is rolled every hour.
- The hourly data is rolled up every day at 12:00 a.m.
- The daily data is purged everyday at 1:00 a.m.

Changing the Number of Records Displayed

Pages may load slowly because of large amounts of data stored for the following reports:

- Event History, page 11-15
- Events, page 11-16
- SNMP Trap Log, page 11-31
- Syslog Entries, page 11-33
- Windows Event Log, page 11-36

You can change the number of records displayed for these reports.

Step 1 Select **GO > Configure > Report Preferences...**.

Step 2 Enter a number from 1 to 10000. The default number of records displayed is 1500.

Note A warning message is shown if the report does not show all the records available for the selected time range.

About System Reports

System reports display system-wide information. System reports do not focus on a particular device or a specific device group, but rather all devices that fall under a certain category. For example, when choosing to view the General Error Log, all errors that occurred on your network are listed, regardless of which group a device belongs to.

When viewing a system report, take note of the features made available to you to enhance your report viewing experience:

- The report Date/Time drop-down list located in the middle of the page allows you to easily change the time period for the report you are viewing.
- The Additional Reports drop-down list allows you to easily jump to other system reports, or to bring up the report selection drop-down list to select from all reports.

  To the right of the Additional Reports drop-down list are the report icons:

  – **Export**—Allows you to export a report into text or Microsoft Excel.

  – **Favorites**—Allows you to add a report to your list of Favorites.

  – **Help**—Brings up the Cisco netManager help system.

About Group Reports

Group reports display information relating to a specific device group. For example, when choosing to view the Group Actions Applied report, you must choose to which group the report applies and can view only Actions applied in that specific group.

When viewing a group report, take note of the features made available to you to enhance your report viewing experience. Along with the Date/Time drop-down list and the report icons available to you when viewing system reports, there are two other features unique to group reports:

- The Additional Reports drop-down list allows you to easily jump to other group reports, or to bring up the report selection drop-down list to select from all reports.
- The All Devices button, located to the right of the Reports tab, brings up the Device Group selection drop-down list dialog. From this dialog you can choose a group for the report you are viewing.

About Device Reports

Device reports display information relating to a specific device. For example, when choosing to view the CPU Utilization report for a specific device, only CPU utilization information is listed for the specific device you choose for the report.

When viewing a device report, take note of the features made available to you to enhance your report viewing experience. Along with the Date/Time drop-down list and the report icons available to you when viewing system and group reports, there are two other features unique to device reports:

- The Additional Reports drop-down list allows you to easily jump to other device reports.
- The Device link located directly to the right of the Reports tab allows you to change the device context for the report you are viewing.
- The Device Properties link located to the right of the Device link brings up the device properties for the device-in-context.

Note If workspace content or report information is not relevant or available for a selected device, the workspace content or report will show no data. For more information about workspace content, see Chapter 3, "Understanding Workspaces and Workspace Content."

About Phone Reports

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

Phone reports contain the following information:

- Phone extension
- Description
- IP address (launch point)
- Mac address
- Phone model
- Registration status with Communications Manager/Communications Manager Express
- Communications Manager/Communications Manager Express address to which phone is registered
- Switch address
- Switch port information
- Switch port status—Status of the switch port used by the IP phone.
- VLAN name—Name of the VLAN used by the IP phone.
- Serial Number—Serial number of the IP phone.

Phone audit and phone move reports are provided.

When viewing a system report, you can enhance your report viewing experience by using the **Additional Reports** drop-down list which allows you to easily jump to other system reports, or to bring up the report selection drop-down list to select from all reports.

To the right of the Additional Reports drop-down list are the report icons:

- **Export**—Allows you to export a report into text or Microsoft Excel.
- **Favorites**—Allows you to add a report to your list of favorites.
- **Help**—Brings up the Cisco netManager help system.

List of Reports

The following tables list all reports that are available in Cisco netManager.

(P) = Performance

(PA) = Problem Areas

(G) = General

Table 11-1 System Reports

Report Name	Details
Action Log (PA)	A record of all Actions that Cisco netManager attempts to fire.
Active Discovery Log (G)	A record of all Active Discovery task results.
Activity Log (G)	A history of system-wide configuration and application initialization messages generated by Cisco netManager for the selected time period.
All IP Phones/Lines	Use the All IP Phones/Lines report to view data for all IP phones and lines discovered in the network that Cisco netManager is monitoring.
Devices Import Status	Device import status.
Devices Reports	Current monitored status of the devices.
Event History	A record of Cisco netManager event history for a group.
Events	A record of all Cisco netManager events for a group.
General Error Log (PA)	A record of error messages generated by Cisco netManager.
Home Workspace	Your home workspace.
IP Phone Audit	All the IP phones and lines in the network that were registered/unregistered/removed.
IP Phone Move	All the IP phones and lines in the network that were moved.
Passive Monitor Error Log (PA)	A record of passive monitor errors reported by Cisco netManager.
Performance Monitor Error Log (PA)	A record of Performance Monitor errors reported by Cisco netManager.
Recurring Action Log (G)	Results of Recurring Action executions.
Recurring Report Log (G)	Results of Recurring Report executions.
Registered Phones Report	Displays all phones registered with a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.
SNMP Trap Log (PA)	A history of SNMP traps that have occurred during the selected time period. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.

Table 11-1 System Reports (continued)

Report Name	Details
State Change Acknowledgement (PA)	When a device state changes, regardless of any action that has been placed on the device, Cisco netManager uses the Acknowledgement feature to make you aware that the state change occurred. This report can be used to view the devices which require acknowledgement and then acknowledge them.
Syslog Entries (PA)	Syslog events logged during the selected time period. If the Syslog Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Syslog Entries log.
Unregistered IP Phones	Displays all phones not registered with a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.
Web User Activity Log (G)	Shows the history of user activity on the system.
Windows Event Log (PA)	Shows Windows events logged for all devices during the selected time period. If the Windows Event Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Windows Event Log.
Wireless LWAP Summary	Wireless lightweight access point inventory details in the system.

Table 11-2 Group Reports

Report Name	Details
Actions Applied (G)	The Group Actions Applied report shows how Actions are applied to devices and monitors in the current group. Each entry shows an action and the device, monitor and state that triggered it.
Active Monitor Availability per Device (PA)	Compare the amount of time the Active Monitors on your devices have been available.
Active Monitor Outage (PA)	Compare the amount of time the Active Monitors on your devices have been down.
CPU Utilization per Device (P)	CPU utilization statistics for devices by group.
Disk Utilization per Device (P)	Disk space utilization statistics for devices by group.
Event History	A record of Cisco netManager event history for a group.
Events	A record of all Cisco netManager events for a group.
Health per Device	The current status of monitored devices in the selected group, along with each monitor configured to those devices.
Interface Utilization per Device (P)	Interface traffic and utilization for devices by group.
IP Phone Audit	All the IP phones and lines in the network that were registered/unregistered/removed.

Table 11-2 Group Reports (continued)

Report Name	Details
IP Phone Move	All the IP phones and lines in the network that were moved.
IP Phones and Lines per Device	All the IP phones/lines discovered in the network for a group.
IP Phones and Lines per Group	All the IP phones/lines discovered in the network for a group.
Memory Utilization per Device (P)	Memory utilization statistics for devices by group.
Ping Availability per Device (P)	Ping availability statistics for devices by group.
Ping Response Time (P)	Ping response times for devices by group.
State Change Acknowledgement	Use this report to acknowledge state changes in Cisco netManager.
State Change Timeline per Device (PA)	A timeline of when each monitor on a device in the selected group changed from one state to another during the selected time period.
State Summary (G)	A summary of device states organized by device group.
Top 10	A collection of Top 10 reports.

Table 11-3 Device Reports

Report Name	Details
Active Monitor Availability per Device (PA)	Find out when the Active Monitors on your device have been accessible.
Chassis Inventory Details	Chassis inventory details.
CPU Utilization per Device (P)	CPU utilization statistics for a device.
Custom Performance Monitors (P)	View information on your devices collected by Performance Monitors.
Device Status (G)	A detailed look at a specific device.
Disk Utilization per Device (P)	Disk space and utilization statistics for a device.
Flash Devices Inventory	Flash devices inventory details.
Flash Files Inventory	Flash files for a device.
Health per Device (PA)	Displays the current status (a snapshot) of the selected device and all monitors on that device. Each monitor shows its own device state, the current status of each item, how long the device has been in that status, and the time that status was first reported.
Interface Details	Displays interface information for the device.
Interface Utilization per Device (P)	Interface traffic and utilization statistics.
IP Phones and Lines per Device	All the IP phones/lines discovered in the network for a group.
IP Phones and Lines per Group	All the IP phones/lines discovered in the network for a group.

Table 11-3 Device Reports (continued)

Report Name	Details
Memory Utilization per Device (P)	Memory utilization statistics for a device.
Module Inventory	Modules inventory details for a device.
Performance Monitor Error Log (PA)	A record of Performance Monitor errors for an individual device.
Ping Availability per Device (P)	Availability statistics for a device.
Ping Response Time (P)	Ping response times for an individual device.
Power Supply Status	Displays the device's power supply status with the last polled time stamp. Displays the device's power supply status with the last polled time stamp. Displays the device's power supply status with the last polled time stamp. Displays the device's power supply status with the last polled time stamp.
SNMP Trap Log (PA)	A history of SNMP traps that have occurred for the selected device during the selected time period. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.
Stack Inventory	Stack inventory details for a device.
State Change Timeline per Device (PA)	This report shows a timeline of when each monitor on the selected device changed from one state to another during the selected time period.
Syslog Entries (PA)	This report shows syslog events logged for the selected device during the selected time period. If the Syslog Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Syslog Entries Log.
Temperature Statistics	This report shows temperature statistics for the device.
Cisco Unity Port Details	A summary of ports associated with the Cisco Unity device. This report is accessible from **Device Status Workspace** > **Additional Reports** only.
Cisco Unity Port Utilization	Port utilization statistics for a Cisco Unity device. This report is accessible from **Device Status Workspace** > **Additional Reports** only.
Voice Gateway Details	This report shows any gateway connectivity details with another device. This report is accessible from **Device Status Workspace** > **Additional Reports** only.
Voice Services Details	This report displays a list of voice services running on the device. This report is accessible from **Device Status Workspace** > **Additional Reports** only.
Windows Event Log (PA)	This report shows Windows events logged for the selected device during the selected time period. If the Windows Event Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Windows Event Log.

Active Discovery Log

This system report shows the results of all active discovery tasks that are configured in Cisco netManager. This log shows the general result of the task, but does not show which devices and services were discovered. You must access the Active Discovery Results report to process the discovered items.

- Date—The date and time that the active discovery task was run.
- Active Discovery—The name of the active discovery task that was run.
- Result—The result of the active discovery task: success, success with results, failure, or disabled. If the result is success with results, you can click the link to process the results of the active discovery task.
- Details—Text that describes the result of the active discovery task.

Active Monitor Availability

When Active Monitor Availability is selected as a group report it displays a summary of availability times for all Active Monitors within a device group. The following information is displayed within the report:

- Device—The network device. Click one of the device entries to view the Device Active Monitor Availability Report for that device.
- Monitor—The type of Active Monitor.
- Up—The percentage for the amount of time the Active Monitor was up.
- Maintenance—The percentage for the amount of time the Active Monitor was in maintenance.
- Unknown—The percentage for the amount of time the Active Monitor was in an unknown state.
- Down—The percentage for the amount of time the Active Monitor was down.
- Availability—The overall availability for the Active Monitor by color.
  - Green—Above 90%.

Active Monitor Availability per Device

When Active Monitor Availability is selected as a device report it displays an area graph that outlines the availability of the selected device's Active Monitors.

At the bottom of the graph, the summary section displays:

- Up—The percentage that represents the amount of time the Active Monitors were up.
- Maintenance—The percentage that represents the amount of time the Active Monitors were in maintenance.
- Unknown—The percentage that represents the amount of time the Active Monitors' status was unknown.
- Down—The percentage that represents the amount of time the Active Monitors were down.
- Availability—The overall availability of the Active Monitors, by color.
  - Green—Above 90%.
  - Yellow—Between 80% and 90%.

Table 11-3 Device Reports (continued)

Report Name	Details
Wireless LWAP Channel Utilization	This report displays wireless lightweight access point channel utilization details for a controller.
Wireless LWAP Summary	This report displays wireless lightweight access point inventory details for a controller.

Action Log

This system report shows all actions that Cisco netManager has attempted to start, based on the configuration of the action.

The following information is displayed in the log:

- Date—The date the action was started.
- Action—The specific action type that was started. This corresponds to the name of the action in the Actions Library.
- Category—Shows the category of the action: success, failure, cancel, retry, or blacked out.
- Device—The device that the action is assigned to.
- Active Monitor—The active monitor that the action is assigned to.
- Passive Monitor—The passive monitor that the action is assigned to.
- Trigger State—The state that caused the action to fire. The trigger state is determined when the Action is configured on the device.
- Details—Text that shows the reason for the category that is used in the log.

Actions Applied

This group report shows how actions are applied to devices and monitors in the current group. Each entry shows an action and the device, monitor and state that triggered it. From this report, click **Select a different group** to access the report for another group.

- Device—The group device.
- State—The state of the action at the time of the last poll, relative to the time selected in the report date/time selector.
- Action type—The type of action applied to the device.
- Action—The action applied to the device.
- Monitor—The type of monitor.

Active Monitor Outage

This group report shows the downtime of all unavailable active monitors in the selected group. Monitors are listed by the device they are associated with.

- Device—This column lists the device state icon, host name, and IP address.
- Monitor—This column lists the active monitor as it appears in the Active Monitor Library.

- Down time—Specifies how long the active monitor has been in the Down state.
- Down count—Specifies how many times the active monitor has gone into the Down state during the specified period.

Activity Log

The Activity Log report is a history of system-wide configuration and application initialization messages generated by Cisco netManager for the time period chosen at the top of the report. All messages found in this log are also written to the Windows Event Log.

Each entry shows the type of activity logged as well as the date, source, category and actual message of the activity.

Click the link above the Type column to group the entries by message severity (Information, Warning, or Error).

All IP Phones/Lines

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

The All IP Phones/Lines report includes all IP phones, including Cisco IP Communicators and Cisco IP phones that are configured for SRST.

By default, these reports display only these columns: Extension, User, IP Address, MAC Address, Model, Regd, CCM, Switch Address, and Port. You can hide these columns and select among additional columns to display.

Chassis Inventory Details

This report displays the following inventory details for a device:

- Physical Index—Chassis index.
- Description—Description of chassis.
- Vendor Type—Type of vendor for the chassis.
- Parent Index—Parent index of chassis.
- Name—Name of the chassis.
- Serial No.—Serial number of the chassis.
- Manufacturer Name—Name of the chassis manufacturer.
- Model Name—Vendor-specified model name of the chassis.
- Chassis Version—Version number of the chassis.
- Slot Capacity—Number of slots in the chassis.
- Free Slots—Number of free slots in the chassis.

CPU Utilization per Group

This group performance report displays CPU utilization percentages collected during the selected time period from the devices in the group identified at the top of the report. You can configure the data collection for your devices through **Device Properties > Reporting and Data Collection > Configure CPU Utilizatio**n.

Report Body

Below the date/time picker is a table showing the total number of devices in the current group that are collecting data for the time period chosen, and the total CPU utilization percentage across those devices.

Below the summary table, the report displays the average CPU utilization percentages collected during the time period:

- Device—The name and IP address of the device.
- Description—The description of the CPU on that device.
- CPU Load—The utilization percentage of the CPU for the selected time period.

CPU Utilization per Device

This device performance report displays CPU utilization percentages collected during the selected time period from the device displayed at the top of the report. You can configure the data collection for this device through **Device Properties - Performance Monitors > Configure CPU Utilization**.

Below the date/time drop-down list is a graph showing the CPU utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below it.

At the bottom of the graph, the report displays the average CPU utilization percentages collected during the time period:

- Min Utilization %—The minimum CPU utilization percentage experienced.
- Max Utilization %—The maximum CPU utilization percentage experienced.
- Avg Utilization %—The average CPU utilization percentage across all sample data for this time period.

The Raw Data table displays all of the data samples that were collected during the time period selected.

Custom Performance Monitors

This device performance report graphs custom performance monitor values over a selected period of time. You can configure the data collection for this device through **Device Properties > Performance Monitors**.

- Monitor—The custom performance monitor chosen for data collection.
- Date/time drop-down list—Select the dates and times for which you want monitoring data.
- Chart size—Select the size you would like the chart to display in.

Below the date/time drop-down list and the Monitor and Chart size boxes is a graph showing the chosen monitor for the selected time period. Each point on the graph corresponds with an entry in the graph data table below it.

At the bottom of the graph the report displays the average monitor percentages collected during the time period:

- Minimum—The minimum monitor percentage experienced.
- Maximum—The maximum monitor percentage experienced.
- Average—The average monitor percentage across all sample data for this period.

Device Status

This report details the current status (a snapshot) of the selected device.

Device details includes:

- Device properties
- Attributes
- SNMP details

Note Attributes and SNMP details appear only if display information if SNMP is enabled.

Performance Monitors

The following sections will only contain data if the performance monitors have been enabled for the selected device. This can be done on **Device Properties > Performance Monitors**.

To expand or collapse these sections, click the Show/Hide button.

Response time, packet loss, and general ping availability information:

- Response time—The average response time of each monitor attached to the device.
- Packet loss—The total number of packets lost throughout the current group.
- Interface Utilization—Current interface information collected from the device/interface listed. Click inside the graph for historical information.
- CPU Utilization—Current CPU utilization percentages. Click inside the graph for historical information.
- Disk space—Current disk utilization. Click inside the graph for historical information.
- Used—The amount of space used on the disk, in GB.
- Free space—The amount of free space on the disk, in GB.
- Memory Utilization—Current physical and virtual memory utilization. Click inside the graph for historical information.
- Used—The amount of memory utilized, in GB.
- Free space—The amount of memory not utilized, in GB.

Devices Import Status

Shows the status of the last executed or current in-progress device import.

- Import ID—Sequence in which the device definition was found in the import file.
- Device Name—Name of the device.

- Status—Device status. It can have one of the following values:
  - Addition successful.
  - Rejected—Due to duplication, invalid action, or the exceeded license limit.
  - Import failed.
  - In Progress.
- Error—If device status is “rejected” or “import failed,” this column will contain a description of the error.

Devices Reports

This reports displays the discovery status for all the devices in the system.

- Device Type—Type of the device.
- Device Name—Name of the device.
- IP Address—IP address of the device.
- Device Capabilities—Indicates the multiple roles that the device is capable of performing. For example, if a device has the capability of being a router and an H323 gateway, the column lists both router and H323 Gateway.
- Status—Device status. It can have one of the following values:
  - Monitored—Device is reachable during discovery and is being polled.
  - Monitoring Suspended—Polling is suspended on the device.
  - Unreachable—The device did not respond to a ping.
- Last Discovered—Displays the time when the device was last discovered or rediscovered and not polled. This time stamp is updated only on initial discovery and successive rediscoveries.

Disk Utilization per Group

This group performance report displays disk utilization percentages collected during the selected time period from the devices in the group that appears at the top of this report. You can configure the data collection for your devices through **Device Properties > Performance Monitors > Configure Disk Utilization**.

Report Body

Below the date/time picker is a table showing the total number of devices in the group collecting data for the time period chosen, and the total amount of disk space that is being used across those devices.

Below the summary table, the report displays the disk space performance information collected during the time period:

- Device—The name of the device in your database.
- Description—The description of the disk that is being reported on.
- Size—The total size of the disk in GB.
- Used—The amount of space used on the disk in GB.
- Free Space—The amount of free space on the disk in GB.
- % Used—The percentage of the total amount of disk space that is in use.

Disk Utilization per Device

This device report displays disk utilization percentages collected during the selected time period from the device displayed at the top of the report. You can configure the data collection for this device through **Device Properties - Performance Monitors > Configure Disk Utilization**.

Below the date/time drop-down list is a graph showing the disk utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below it.

At the bottom of the graph, the report displays the average disk utilization percentages collected during the time period:

- Total Size—The size of the disk being monitored.
- Min Used—The minimum amount of disk space used.
- Max Used—The maximum amount of disk space used.
- Avg Used—The average amount of disk spaced in use during the time period.
- Min Utilization %—The minimum disk utilization percentage experienced.
- Max Utilization %— The maximum disk utilization percentage experienced.
- Avg Utilization %—The average disk utilization percentage across all sample data for this time period.

The Raw Data table displays all of the data samples that were collected during the selected time period. The data for this report follows the roll-up settings in Program Options - Report Data, so raw data that has already been rolled up to hourly is replaced by an hourly entry in this table. Each entry in this table corresponds to a point in the report graph.

Event History

The event history is a record of the event lifecycle. It contains an entry for when the event was first active. An entry is displayed when the event is acknowledged and when it is cleared.

Note The Events report consolidates the different error conditions of the managed devices into a single viewable format. It displays details such as event name, severity, first raised timestamp, last updated timestamp (by poller/topology/SNMP traps/active monitors), status (active/acknowledged), the component on which the event is raised, and the attributes of that event. For more information, see Events.

The Event History report includes the following fields:

- Severity—Icon depicting severity level of event (critical, warning, or informational).
- Device—Device name or IP address.
- Event Name—Cisco netManager event name.
- Component—Device element on which the event occurred.
- Date—Date and time when the event was generated.
- Attributes—Details the event attributes, for example threshold values.
- State—Event status, based on last polling:
  - Active—Event is live.

  - Cleared—Event is no longer live. Also, when a device is suspended, all alerts are cleared.
  - Acknowledged—Event has been acknowledged.

Events

Events can be raised by functions in Cisco netManager; for example:

- Performance poller
- Health poller
- Logical topology
- SNMP traps
- Active monitors

Events consolidate the different error conditions of the managed devices into a single viewable format. These can be viewed in the device, group, or system reports. An overview of the events can be viewed from the device problem area, which shows the Top 10 list of events in the workspace content view. Click the events in the workspace content to view the report.

An event report can display event details such as event name, severity, first raised timestamp, last updated timestamp (by poller/topology/SNMP traps/active monitors), status (active/acknowledged), the component on which the event is raised, and the attributes of that event.

For each event, the Event report includes:

- Severity—Icon depicting severity level of event (critical, warning, or informational).
- Device—Device name or IP address.
- Event Name—Cisco netManager event name.
- Component—Device element on which the event occurred.
- First Raised Time—Date and time when the event was generated.
- Last Updated Time—Last updated timestamp by poller/topology/SNMP traps/active monitors.
- Attributes—Details the event attributes, for example threshold values.
- State—Event status, based on last polling:
  - Active—Event is live.
  - Acknowledged—Event has been acknowledged.

Flash Devices Inventory

This report displays the following flash file inventory details for a device:

- Index—Flash device index
- Description—Description of flash file.
- Size—Total size of the flash device.

Flash Files Inventory

This report shows the names of flash files for a device.

Fan Status

This report shows the latest poll status of all the fans on the device at the time of the last poll. This is a mini-report.

General Error Log

This system report shows a list of error messages generated by Cisco netManager for the desired time period. Click the column header to change the order and organization of the messages listed.

The following is a list of the type of errors that are logged by this report:

- All errors due to SQL statement failure
- Recurring Report Load error
- Engine startup errors (Device Load error, Group Load error)
- Statistics update error
- State update error
- Roll-up activity and failure
- Device or monitor deletion error
- Exception thrown (check service, process internal event)
- Passive monitor startup errors

Note Events that are reported in this log should be reported to Cisco Systems. They may indicate an application error or bug.

Health

Below the date/time picker is a table showing the total number of devices in the group collecting data for the time period chosen, and the status of the monitors configured for the devices in that group.

Below the summary table, the report displays group status information collected during the time period:

- Device—The network device.
- Monitor—The specific monitor.
- State—The state of the monitor at the time of the last poll for the selected period on the date/time picker.
- How long—The period of time that the monitor has been in the current state.
- When—The date and time the monitor went in to the current state.

Note When exporting this report, an extra column is added to the report which is the same as the existing How long column, but the time is displayed in seconds rather than minutes and hours.

Use the date/time drop-down list at the top of the report to select a date range.

Health per Device

This report displays the current status (a snapshot) of the selected device and all monitors on that device. Each monitor shows its own device state, the current status of each item, how long the device has been in that status, and the time that status was first reported.

For more information about what each icon state means, see "Device States and Icons" section on page 2-4.

Home Workspace

Home workspace reports display in Home workspaces, such as the default Home workspace.

Interface Details

This device report displays the interfaces for the device:

- Description—Lists the description of the interface on the device.
- IP address—IP address of interface.
- VLAN Name—VLAN name the interface belongs to.
- Type—Lists the type of interface on the device.
- MTU—Displays the MTU size.
- Speed—Displays the speed (Mbps).
- Physical Address—Displays the physical address assigned to the interface.
- Administrative State—Possible values for the administrative status of the interface are:
  - Up (green)—Administratively up
  - Down (blue)—Administratively down
  - Testing (blue)—Administrator is testing the interface
- Operational State—Possible values for the operational status of the interface are:
  - Unknown (red)—Unknown operational status.
  - Up (green)—Interface is up.
  - Down (red)—Interface is down.
  - Testing (blue)—Interface is in test mode.
  - Dormant (red)—Interface is dormant.
  - Not Present (red)—Interface component is missing.
  - Lower Layer Down (red)—Interface is down because of a lower-layer interface.

Only the following interface types are displayed:

Interface Type	IfType (MIB2 SNMP Type)
ethernetCsmacd	6
DS1	18

Interface Type	IfType (MIB2 SNMP Type)
basicISDN	20
primaryISDN	21
DS3	30
FrameRelay - DTE only	32
FrameRelayService	44
Fast Ethernet (100BaseT)	62
ISDN and X.25	63
Fast Ethernet (100BaseFX)	69
ISDN S/T interface	75
ISDN U interface	76
Link Access Protocol D	77
Digital Signal Level 0	81
frameRelayMPI - (Multiproto Interconnect over FR)	92
ADSL (Asymmetric Digital Subscriber Loop)	94
RADSL (Rate-Adapt. Digital Subscriber Loop)	95
SDSL (Symmetric Digital Subscriber Loop)	96
VDSL (Very H-Speed Digital Subscrib. Loop)	97
voice recEive and transMit	100
voice Foreign Exchange Office	101
voice Foreign Exchange Station	102
voice encapsulation	103
voice over IP encapsulation	104
Gigabit Ethernet	117
H323 Gatekeeper	164
H323 Voice and Video Proxy	165
MPLS	166
Facility Data Link 4Kbps on a DS1	170
voice E&M Feature Group D	211
voice FGD Exchange Access North American	212
voice Direct Inward Dialing	213

Interface Utilization per Group

This report displays interface utilization information collected during the selected time period from the device/interface in the group that appears at the top of the report. You can configure the data collection for your interfaces through **Device Properties > Performance Monitors > Configure Interface Data Collection**.

Report Body

Below the date/time drop-down list is a table showing interface utilization across the current group for the selected time period.

- Device—The name and IP address of the device.
- Description—The label for the interface being shown.
- Transmit %—The percentage of available bandwidth used by this interface in transmitting data.
- Receive %—The percentage of available bandwidth used by this interface in receiving data.
- Avg. Transmit—The average number of kilobits transmitted through the interface.
- Avg. Receive—The average number of kilobits received through the interface.
- Transmit—The total number of kilobits transmitted through the interface.
- Receive—The total number of kilobits received by the interface.

Interface Utilization per Device

This device performance report displays interface utilization information collected during the selected time period from the device or interface displayed at the top of the report. You can configure the data collection for this interface through **Device Properties - Performance Monitors > Configure Interface Data Collection**.

Below the date/time drop-down list is a graph showing interface utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below. In octets are graphed with an orange line, while out octets are graphed using blue.

At the bottom of the graph, the report displays the average interface utilization collected during the time period:

- Min—The minimum bits-per-second rate experienced on the interface.
- Max—The maximum bits-per-second rate experienced on the interface.
- Avg—The average bits-per-second rate experienced on the interface during the time period.
- Min Utilization %—The minimum interface utilization percentage experienced.
- Max Utilization %—The maximum interface utilization percentage experienced.
- Avg Utilization %—The average interface utilization percentage across all sample data for this time period.

The Raw Data table displays all of the data samples that were collected during the time period previously selected.

Note If a server (for example, Windows 2000 server) has two interface cards, then the interface index number will change each time its Network Connection is disabled and enabled. If you configure an interface performance monitor that collects data for specific interfaces on a device that runs Windows OS and has two interface cards, you need to reconfigure the interface performance monitor after the interface card's index number is changed. The interface index number change is not detected dynamically when the interface statistical monitor is configured to collect data for specific interfaces.

IP Phone Audit

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

Use the IP Phone Audit report to obtain a summary of changes, including data for phones that have been moved or removed, undergone an extension number change, appeared in inventory with a duplicate MAC or IP address, or become suspect.

The IP Phone Audit report shows the changes that have occurred in the managed IP phone network. For example, this report shows you the IP phones that have been added to or deleted from your network, or changes in IP phone status. Phone status changes occur, for instance, when a phone becomes unregistered.

You can see what has changed within the last 7 days. Audits are maintained in the database for a period of 7 days, after which they are purged.

Information for the IP Phone Audit report is gathered by IP Phone Movement Tracking. IP Phone Movement Tracking runs every 5 minutes, so you can run the IP Phone Audit report and obtain fresh data about once every 5 minutes. This interval is not configurable.

The IP Phone Audit report displays the following information:

- Extension—Extension number of the IP phone.
- Serial Number—Serial number of the IP phone.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- CCM Address—Cisco Unified CallManager or Cisco Unified CallManager Express address.
- Switch Name—IP address of the switch to which the IP phone is connected.
- Switch Port—Switch port used by the IP phone.
- Time—Time of audit.

Note Audit date and time are taken directly from Cisco Unified CallManager without adjustment for time zone differences, if any exist, between Cisco Unified CallManager and Cisco netManager systems.

- Audit Type—One of the following:
  - add—Phone added to the network.
  - remove—Phone removed from the network.
  - unregistered—From Cisco Unified CallManager.
  - registered—With Cisco Unified CallManager.

IP Phone Audit Report per Device

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

All the IP phones and lines that were registered, unregistered, or removed in the network for a device

The IP Phone Audit report per device displays the following information:

- Extension—Extension number of the IP phone.
- Description—Description of the IP phone.
- IP address—IP address of the IP phone.
- MAC address—MAC address of the IP phone.
- Serial Number—Serial number of the IP phone.
- Model—Model Number of the IP phone.
- Phone status—Status of the IP phone.
- Switch name—Name of the switch to which the IP phone is connected.
- Port name—Name of the port used by the IP phone.
- Port status—Status of the port used by the IP phone.
- VLAN name—Name of the VLAN used by the IP phone.

IP Phone Audit Report per Group

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

All the IP phones that were registered, unregistered, or removed in the network for a group.

The IP Phone Audit report per group displays the following information:

- Extension—Extension number of the IP phone.
- Serial Number—Serial number of the IP phone.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- CCM Address—Cisco Unified CallManager address.
- Switch Name—Name of the switch to which the IP phone is connected.
- Switch Port—Switch port used by the IP phone.
- Time—Time of audit.
- Audit Type—One of the following:
  - add—Phone added to the network.
  - remove—Phone removed from the network.
  - unregistered—From Cisco Unified CallManager.

– registered—With Cisco Unified CallManager.

IP Phone Move

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

The IP Phone Move report displays IP phones that have moved, including details about the phone before and after the move. The IP Phone Move report shows the time at which the IP phone move was detected, and not the time at which the move occurred.

Information for the IP Phone Move report is gathered every 5 minutes by IP Phone Movement Tracking. IP Phone Movement Tracking checks all the switches and Cisco Unified CallManagers, identifies the list of changes, and generates the data on IP phone moves.

Note You obtain fresh data for the IP Phone Move report about once every 5 minutes. Click **Refresh** to refresh the data.

The IP Phone Move report displays the following details:

- Old Phone Number—Extension number of the IP phone before it was moved.
- New Phone Number—Extension number of the IP phone after it was moved.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- Old CCM Address—Cisco Unified CallManager address of the IP phone before it was moved.
- New CCM Address—Cisco Unified CallManager address of the IP phone after it was moved.
- Old Switch Address—IP address of the switch to which the IP phone was connected before it was moved.
- New Switch Address—IP address of the switch to which the IP phone is connected after it was moved.
- Old Switch Port—Switch port used by the IP phone before it was moved.
- New Switch Port—Switch port used by the IP phone after it was moved.
- Delete Time—Reflects the date and time that Cisco netManager detected the IP phone move.
- Add Time—Reflects the date and time that Cisco netManager detected the new IP phone.

IP Phone Move Report per Device

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

This report details the movement of IP phones or lines in the network for a particular device.

The IP Phone Move report for a device displays the following information:

- OldPhoneNumber—Number of the IP phone before it was moved.
- NewPhoneNumber—Number of the IP phone after it was moved.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- OldCCMAddress—CCM address of the IP phone before it was moved.
- NewCCMAddress—CCM address of the IP phone after it was moved.
- OldSwitchAddress—Switch address used by the IP phone before it was moved.
- NewSwitchAddress—Switch address used by the IP phone after it was moved.
- OldSwitchPort—Switch port used by the IP phone before it was moved.
- NewSwitchPort—Switch port used by the IP phone after it was moved.
- Delete Time—Reflects the date and time that Cisco netManager detected the IP phone move.
- Add Time—Reflects the date and time that Cisco netManager detected the new IP phone.

IP Phone Move Report per Group

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

This report details the movement of IP phones or lines in the network for devices belonging to the selected group.

The IP Phone Move report for a group displays the following information:

- Old Phone Number—Number of the IP phone before it was moved.
- New Phone Number—Number of the IP phone after it was moved.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- Old CCM Address—CCM address of the IP phone before it was moved.
- New CCM Address—CCM address of the IP phone after it was moved.
- New Switch Address—Switch address used by the IP phone after it was moved.
- Old Switch Port—Switch port used by the IP phone before it was moved.

IP Phones and Lines per Device

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

All the IP phones and lines discovered in the network for a device.

The IP phone report for a device displays the following information:

- Extension—Extension number of the IP phone.

- Description—Description of the IP phone.
- IP address—IP address of the IP phone.
- MAC address—MAC address of the IP phone.
- Serial Number—Serial number of the IP phone.
- Model—Model number of the IP phone.
- Phone status—Status of the IP phone.
- Switch name—Name of the switch to which the IP phone is connected.
- Port name—Name of the port used by the IP phone.
- Port status—Status of the port used by the IP phone.
- Vlan name—Name of the VLAN used by the IP phone.

IP Phones and Lines per Group

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

All the IP phones/lines discovered in the network for a group.

The IP Phone report for a group displays the following information:

- Extension—Extension number of the IP phone.
- Description—Description of the IP phone.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- Serial Number—Serial number of the IP phone.
- Model—Model number of the IP phone.
- CCM Name—CCM address of the IP phone.
- Switch name—Name of the switch to which the IP phone is connected.
- Port name—Name of the port used by the IP phone.
- Port status—Status of the port used by the IP phone.
- Vlan name—Name of the VLAN used by the IP phone.

Memory Utilization per Group

This group report displays memory utilization data collected during the selected time period from the devices in the group shown at the top of the report. You can configure the data collection for your devices through **Device Properties > Performance Monitors > Configure Memory Utilization**.

Report Body

Below the date/time picker is a table showing the total number of devices in the group that are collecting data for the time period chosen, the total amount of memory that is available, and the amount that is was in use across those devices.

Below the summary table, the report displays the memory utilization data collected during the time period:

- Device—The name and IP address of the device.
- Description—The description of the type of memory on that device.
- Size—The total amount of memory on the device being monitored.
- Used—The amount of memory in use on the device.
- % Used—The utilization percentage of the memory for the device.

Memory Utilization per Device

This device performance report displays memory utilization collected during the selected time period from the device displayed at the top of the report. You can configure the data collection for this device through **Device Properties - Performance Monitors > Configure Memory Utilization**.

Below the date/time drop-down list is a graph showing the memory utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

At the bottom of the graph, the report displays the average memory utilization collected during the time period:

- Total Size—The total amount of memory on the device being monitored.
- Min Used—The minimum amount of memory in use on the device.
- Max Used—The maximum amount of memory in use on the device.
- Avg Used—The average amount of memory in use on the device during the time period.
- Min Utilization %—The minimum disk utilization percentage experienced.
- Max Utilization %— The maximum disk utilization percentage experienced.
- Avg Utilization %—The average disk utilization percentage across all sample data for this time period.

The Raw Data table displays all of the data samples that were collected during the time period selected above. The data for this report follows the roll-up settings in Program Options- Report Data, so raw data that has already been rolled up to hourly is replaced by an hourly entry in this table. Each entry in this table corresponds to a point in the report graph.

Module Inventory

This report displays the following module details:

- Physical Index—Physical index of module.
- Description—Description of module.
- Vendor Type—Type of vendor for module.
- Parent Index—Parent index of module.
- Parent Type—Parent type of module.
- Name—Name of module.
- Serial No.—Serial number of module.
- Manufacturer Name—Manufacturer name of module.

- Model Name—Model name of module.
- Operational Status—Current operational status.
- Administrative Status—Current administrative status.
- Module IP Address—IP address of module.
- Module Index—Index of module.
- Slot Num.—Slot number of module.
- Num. of Port—Number of ports in module.
- Last Poll Time—Time module was last polled for operational and administrative status.

Passive Monitor Error Log

This system problem areas report shows all passive monitor errors that occur during the operation of Cisco netManager.

Below the date/time drop-down list is a table showing all passive monitor errors that occurred during the time period chosen.

Below the summary table, the report displays system-wide information collected during the time period:

The following information is displayed in the log:

- Date—The date of the error.
- Passive Monitor—The name of the passive monitor that received the error.
- Device—The host name of the device that the passive monitor is assigned to.
- Category—The category code of the error: Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error).
- Details—Text that describes the error that was received.

Performance Monitor Error Log

When Performance Monitor Error Log is selected as a system problem areas report, it shows all Performance Monitor errors that occur during the operation of Cisco netManager.

The following information is displayed in the log:

- Date—The date of the error.
- Category—The category of the error.
- Source—Where the error came from (such as Ping, CPU, Memory, Disk, Interface, and Custom Performance Monitors).
- Details—Text that describes the error that was received.
- Device—The host name of the device that the Performance Monitor is assigned to.

When Performance Monitor Error Log is selected as a device problem areas report, it shows all Performance Monitor errors that occur during the operation of Cisco netManager for a specified device.

The following information is displayed in the log:

- Date—The date of the error.
- Category—The category of the error.

- Source—Where the error came from (such as Ping, CPU, Memory, Disk, Interface, and Custom Performance Monitors).
- Details—Text that describes the error that was received.

Ping Availability

This performance report displays ping availability data collected during the selected time period from the device group displayed at the top of the report. You can configure the data collection for individual devices through **Device Properties > Performance Monitors > Configure Ping Latency and Availability**.

- Packets Sent—The total number of packets sent throughout the current group during the selected time period.
- Packets Lost—The total number of packets lost throughout the current group during the selected time period.
- Percent Packet Loss—A percentage of packet loss throughout the current group for the selected time period.
- Total Poll Time (minutes)—Total amount of time (in minutes) that passed during the time period selected.
- Time Unavailable (minutes)—Total amount of time (in minutes) that a device was unavailable in the group.
- Percent Available—The total availability percentage averaged over all samples during the selected time period.

The Device Data table displays the same information as above, but on a per device basis.

Ping Availability per Device

This device performance report displays ping availability data collected during the selected time period from the device displayed at the top of the report.

Below the date/time drop-down list is a graph showing device ping availability for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

At the bottom of the graph, the report displays general ping availability information for the device collected during the selected time period:

- Packets Sent—The total number of packets sent from the device during the selected time period.
- Packets Lost—The total number of packets lost from the device during the selected time period.
- Poll Time (minutes)—Amount of total time (in minutes) that passed during the time period selected.
- Time Unavailable (minutes)—Amount of total time (in minutes) that the device was unavailable in the group.
- Percent Available—The total availability percentage for the device.

The Raw Data table displays all of the data samples that were collected during the time period selected above. The data for this report follows the roll-up settings in Program Options. Report Data (in the Cisco netManager console), so raw data that has already been rolled up to hourly is replaced by an hourly entry in this table. Each entry in this table corresponds to a point in the report graph.

Ping Response Time

This group performance report displays ping response time data collected during the selected period from the device group displayed at the top of the report. This is the amount of time it takes a packet to be returned from the device after an Internet Control Message Protocol (ICMP) poll.

Below the list of devices in the current group, the Summary table shows the average response time for all interfaces in the group.

- Device—The device the ping monitor is active on.
- Interface—The specific interface the ping monitor is active on.
- Min response time (ms)—The minimum ping response time (in milliseconds) experienced for the device during the selected time period
- Max response time (ms)—The maximum ping response time (in milliseconds) experienced for the device during the selected time period.
- Avg response time (ms)—The average ping response time (in milliseconds) experienced for the device across all sample data for this time period.

Ping Response Time per Device

This report displays ping response time data collected during a period of time.

- Device—The device the ping monitor is active on.
- Interface—The specific interface the ping monitor is active on.
- Min response time (ms)—The minimum ping response time (in milliseconds) experienced for the device during the selected time period
- Max response time (ms)—The maximum ping response time (in milliseconds) experienced for the device during the selected time period.
- Avg response time (ms)—The average ping response time (in milliseconds) experienced for the device across all sample data for this time period.

Power Supply Status

This is a mini-report. It displays the device's power supply status with the last polled time stamp:

- Description—Description of the power supply.
- Status—Power supply status.
- Last Poll Time—Time power supply status was last polled.

Recurring Action Log

Use this system-wide general report to view the results of recurring actions that were scheduled to fire.

- Recurring Action—The name of the recurring action that was scheduled to fire.
- Date—The date and time the attempt to fire the action occurred.
- Category—The result of the attempt to fire the action (success, failure, information, or cancel).

- Details—This column displays information about the specific action that was scheduled to fire. If the category is information, details show that the scheduled action occurred during a blackout period. If the category is cancel, details show that the action was stopped while it was in the process of being fired, either manually by the user or by the shutdown of the Cisco netManager Engine service.

Recurring Report Log

This general system report shows a log of all recurring reports that have occurred during the selected time period.

The following information is displayed in the log:

- Recurring Report—The name of the recurring report as is appears on the Recurring Report dialog.
- Date—The date that the report was run.
- Category—The result of the report attempt: Success, Failure, Disabled.
- Details—Describes the results of the report.

Registered Phones Report

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

The Registered Phone Report displays the number of registered phones in the network and contains the following details:

- Extension—Extension number of the IP phone. The Extension column has two subcolumns:
  - Old—Extension number of the IP phone before it was moved.
  - New—Extension number of the IP phone after it was moved.
- Description—Description of the IP phone.
- IP Address—IP address of the IP phone.
- MAC Address—MAC address of the IP phone.
- Serial Number—Serial number of the IP phone.
- Model—Model number of the IP phone.
- Phone status—Status of the IP phone.
- Switch name—Name of the switch to which the IP phone is connected.
- Port name—Name of the port used by the IP phone.
- Port status—Status of the port used by the IP phone.
- Vlan name—Name of the VLAN used by the IP phone.

SNMP Trap Log

When SNMP Trap Log is selected as a system report, it provides a history of SNMP traps that have occurred for all devices on the network during the time period displayed at the bottom of the report. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.

Note For entries to be added to this report, the SNMP Trap Listener must be enabled. For more information, see Enable the SNMP Trap Handler, page 9-3.

- Date—The date the SNMP trap was received by Cisco netManager.
- Source—The device or program that originated the trap.
- Trap—The type of trap that was received.
- Payload— The vital data (such as the trap name, the IP address that the trap came from, date of the trap, and so on) that is passed within a packet or other transmission unit. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the payload, click the payload entry to launch the Payload Viewer.

SNMP Trap Log per Device

When SNMP Trap Log is selected as a device report, it provides a history of SNMP traps that have occurred for the selected device during the time period displayed at the bottom of the report. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.

Note For entries to be added to this report, the SNMP Trap listener must be enabled and an SNMP Trap passive monitor must be added to the device. For more information, see Enabling the SNMP Trap Listener.

- Date—The date and time the trap occurred.
- Trap—The type of trap.
- Payload—The vital data (such as the event name, the IP address that the event came from, date of the event, and so on) that is passed within a packet or other transmission unit. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to launch the Payload Viewer.

Stack Inventory

This report displays the following stack information for a device:

- Physical Index—Physical index of stack.
- Description—Description of stack.
- Vendor Type—Type of vendor for the stack.
- Parent Index—Parent index of the stack.
- Name—Stack name.

- Serial No.—Serial number of the stack.
- Manufacturer Name—Manufacturer name of the stack.
- Model Name—Model name of the stack.

State Change Acknowledgement

When a device state changes, regardless of any action that has been placed on the device, Cisco netManager uses the Acknowledgement feature to make you aware that the state change occurred. This report can be used to view the devices which require acknowledgement and then acknowledge them.

State Change Timeline per Group

This group report shows a timeline of when each monitor on a device in the selected group changed from one state to another during the selected time period.

- Start time—The date and time of the state change.
- Device-Monitor—The device name and the type of monitor that experienced the state change.
- State—The state of the condition at the time of the poll. The thin gray bar on a state indicator color block means that the device state change has not been acknowledged.
- Duration—The amount of time the state remained unchanged.
- Message—The actual result message returned to Cisco netManager at the time of the poll.

Click a device entry to access the Device Status Report for that device.

State Change Timeline per Device

This device report displays a time line of when each monitor on a device changed from one state to another during the selected time period.

The following information is displayed within the report:

- Start time—The date and time of the state change.
- Monitor—The type of monitor that experienced the state change.
- State—The state of the condition at the time of the poll. The thin gray bar on a state indicator color block means that the device state change has not been acknowledged.
- Duration—The amount of time the state remained unchanged.
- Message—The actual result message returned to Cisco netManager at the time of the poll.

Note At first glance, you may feel the report is displaying incorrect information. For example, you might select the time period to be today or yesterday but see a date that occurred last week or even last month. This happens because the monitor is still in the same state today as it was in a few days or weeks ago, or even a month before.

Use the date/time drop-down list at the top of the report to select a date range.

State Summary

This group report is a summary of device states in the current selected group.

The top section of the report shows the number of Devices Up, Devices Down, Devices in Maintenance, Monitors Up, and Monitors Down. Click the number to view a list of devices that match that device state.

Click expand or contract on the Group Summary to show or hide the subgroups within the current groups shown.

The bottom section shows a list of the items that correspond to the number at the top of the report.

Click the device name to launch the Device Properties for that device.

Syslog Entries

This report shows Syslog events logged for all devices on the network during the time period displayed at the top of the report.

Note For entries to be added to this report, the Syslog listener must be enabled. For more information, see Using the Passive Monitor Library, page 9-2.

A Syslog event is used to examine Syslog messages forwarded from other devices for a specific record and/or specific text within a record. Usually Syslog messages are forwarded from the Syslog on a system that runs UNIX, but they can also come from non-UNIX devices as well. They might contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.

The Syslog Entries report is organized into a list and divided into the following columns:

- Date—The date the Syslog entry was received by Cisco netManager.
- Device—The device or program that originated the entry.
- Syslog Type—The type of Syslog entry that was received.
- Payload—The vital data that is passed within a packet or other transmission unit. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to launch the Payload Viewer.

Syslog Entries per Device

When Syslog Entries is selected as a device report, it displays disk utilization percentages collected during the selected time period from the device displayed at the top of the report. You can configure the data collection for this device through **Device Properties - Performance Monitors > Configure Disk Utilization**.

Below the date/time drop-down list is a graph showing the disk utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

At the bottom of the graph, the report displays the average disk utilization percentages collected during the time period:

- Total Size—The size of the disk being monitored.
- Min Used—The minimum amount of disk space used.
- Max Used—The maximum amount of disk space used.

- Avg Used—The average amount of disk spaced in use during the time period.
- Min Utilization %—The minimum disk utilization percentage experienced.
- Max Utilization %— The maximum disk utilization percentage experienced.
- Avg Utilization %—The average disk utilization percentage across all sample data for this time period.

The Raw Data table displays all of the data samples that were collected during the time period selected above. The data for this report follows the roll-up settings in Program Options - Report Data, so raw data that has already been rolled up to hourly is replaced by an hourly entry in this table. Each entry in this table corresponds to a point in the report graph.

Temperature Statistics

Displays a graph showing the temperature (in degrees) during specified intervals.

Top 10

A collection of reports that focus on the current health of your network devices. It is preconfigured to include workspace reports that display data on the top network devices by:

- Interface utilization
- Interface traffic
- Ping response time
- Disk utilization
- CPU utilization
- Memory Utilization

Cisco Unity Port Details

This report displays Cisco Unity port information:

- Phone System—The phone system integration to which this port belongs. This could be cisco callmanager or a traditional PBX.
- Messaging Port #—The voice messaging port number.
- is Trap connection—Indicates whether this port is designated for use by subscribers as a Telephone Recording And Playback (TRAP) device in Cisco Unity web applications and e-mail clients.
- is AMIS delivery?—Indicates whether this port is designated for making outbound AMIS calls to deliver voice messages from Cisco Unity subscribers to users on another voice messaging system.
- is MWI port—Indicates whether this port is designated for turning MWIs on and off.
- is incoming answer?—Indicates whether this port is designated to answer incoming calls.
- is message notifier?—Indicates whether this port is designated for notifying subscribers of messages.
- Status—Indicates whether this port is enabled on the local Cisco Unityserver.

Cisco Unity Port Utilization

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

This device performance report displays Cisco Unity Port utilization collected during the selected time period from the device displayed at the top of the report. Select Port type information and configure the data collection for this device through **Device Properties - Performance Monitors > Configure Unity Port Utilization**.

Below the date/time drop-down lists is a graph showing the memory utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

At the bottom of the graph, the report displays the average port utilization collected during the time period:

- Min Utilization %—The minimum port utilization percentage experienced.
- Max Utilization %— The maximum port utilization percentage experienced.
- Avg Utilization %—The average port utilization percentage across all sample data for this time period.

Unregistered IP Phones

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

This report displays all phones that are not registered with a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

Voice Gateway Details

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

This report shows details of any gateway connectivity with another device:

- Name—Name of device associated with this gateway.
- IP Address—IP address of device.
- Status—Device status.

Voice Services Details

Note The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

This report shows any services running on the device.

- Product Name—Name of service running on the device.
- Version—Software version running on the device.
- State—Device status.

Web User Activity Log

This log records when a user logs in or out of the web interface, and the actions taken while logged in.

Windows Event Log

When Windows Event Log is selected as a system problem areas report, it shows Windows events logged for all devices during the time period displayed at the bottom of the report.

Note For entries to be added to this report, the Windows Event Log listener must be enabled. For more information, see Using the Passive Monitor Library, page 9-2.

A Windows log event is a Windows Event Viewer entry monitored by Cisco netManager. It could be monitoring when a service is started or stopped, if there was a logon failure, or any other entry in the Windows Event Viewer.

- Date—The date the event was received by Cisco netManager.
- Source—The device or program that originated the entry.
- WinEvent Type—The type of message received.
- Payload—The vital data (such as the event name, the IP address that the event came from, the date of the event, and so on) that is passed with the event message. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to launch the Payload Viewer.

Windows Event Log per Device

When Windows Event Log is selected as a device problem areas report, it shows Windows events logged for the selected device during the time period displayed at the bottom of the report.

Note For entries to be added to this report, the Windows Event Log listener must be enabled and a Windows Event passive monitor must be added to the device.

A Windows log event is a Windows Event Viewer entry monitored by Cisco netManager. It could be monitoring when a service is started or stopped, if there was a logon failure, or any other entry in the Windows Event Viewer.

- Date—The time the event was received by Cisco netManager.
- WinEvent Type—The type of message received.
- Payload—The vital data (such as the event name, the IP address that the event came from, the date of the event, and so on) that is passed within a packet or other transmission unit. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to launch the Payload Viewer.

Wireless LWAP Summary

This report displays wireless lightweight access point inventory details in the system:

- AP ID—Access point ID.
- AP Name—Name of access point.
- Ethernet MAC Address—Ethernet MAC address of access point.
- IP Address—IP address of access point.
- Operational Status—Current operational status.
- Administrative Status—Current administrative status.
- Connected to Device - Name(s)—Names of CDP neighbors of the access point.
- Connected to Device - IP Address(es)—IP addresses of CDP neighbors of the access point.
- No. of Users—Total number of users associated with all the radios on the access point.
- IOS Version—Cisco IOS software version of access point.
- Boot Version—Boot version of access point.
- No. of Radio Interfaces—Number of radio interfaces of access point.
- Model—Model name of access point.
- Serial No.—Serial number of access point.
- Controller Port No.—Port on the controller on which this access points traffic is coming through.
- Location—Location of access point.
- Last Poll Time—Time when operational and administrative status was last polled.
- Associated to Controller (available in system reports).

Wireless LWAP Channel Utilization

The Wireless LWAP Channel Utilization report depicts the channel utilization of the lightweight access points registered with the Wireless LAN Controller. The utilization data is represented as a graph, for each of the radio interfaces on the access points. Select an access point interface from the drop-down list.

Printing, Exporting, and Saving Reports

All reports can be printed and many can be exported into text or Microsoft Excel. For either the print or export functions to work, client-side JavaScript must be enabled. Reports can also be saved for later review.

To print a full report while viewing the full report you want to print:

Step 1 Right-click anywhere inside the report window.

Step 2 From the right-click menu, select **Print.**

Step 3 Do one of the following:

- On the Print dialog, click **Print.**
- Select **File** > **Print**.

Step 4 On the Print dialog, click **Print.**

To export a full report to text while viewing the full report you want to export:

Step 1 On the Report Toolbar, click the **Export** button.

Step 2 On the Export Report dialog, select **Export to Text**.

Step 3 To either include or remove the report title or column names from the exported file, clear or select the following options:

- **Include report title**
- **Include column names**

Step 4 Choose a **Column delimeter** from the drop-down menu.

Step 5 Choose a **Text qualifier** from the drop-down menu.

Step 6 Click **OK** to export the report to text.

To export a full report to Microsoft Excel while viewing the full report you want to export:

Step 1 On the Report Toolbar, click the **Export** button.

Step 2 On the Export Report dialog, select **Export to Excel**.

Step 3 To either include or remove the report title or column names from the exported file, clear or select the following options:

- **Include report title**
- **Include column names**

Step 4 Click **OK** to export the report to Excel.

To save a full report:

Step 1 While viewing the full report you want to save, select **File > Save As**.

Step 2 In the Save Web Page dialog, browse to the location to which you want to save your file from the **Save in** box.

Step 3 Give the file a name in the **File name** box.

Step 4 Choose the type of file you want to save the report as from the **Save as type** box.

Step 5 Click **Save.**

Date/Time Drop-Down List

Use the date/time drop-down list at the top of the report to select a date range.

Zoom Tool

Use the zoom tool to navigate through a report. The zoom tool will change the date and time of a report as you page up and down, or zoom in and out:

- Page up—Moves the report date forward. For example, clicking the Page up button will move the date from today to tomorrow.
- Zoom in—Decreases the amount of time displayed in the report. For example, click the Zoom in button will decrease the display time from 24 hours to 12 hours.
- Zoom out —Increases the amount of time displayed in the report. For example, clicking the Zoom out button will increase the display time from 12 hours to 24 hours.
- Page down—Moves the report date backward. For example, clicking the Page down button will moved the date from today to yesterday.

Adding a Report to Your List of Favorites

As you view reports, you may find that you tend to visit certain reports more than others. Cisco netManager allows you to save these reports to your list of favorites so that you can easily navigate to them.

To add a report to your list of favorites:

Step 1 Select a report to view from the Cisco netManager Reports tab.

Step 2 Click the **Favorites** button located in the upper right side of the report page.

To remove a report from your list of favorites:

Step 1 Navigate to your list of favorites from the Report Overview page.

Step 2 Click the **Remove** button next to the report(s) you want to remove from your list of favorites.

Using Recurring Reports

Through this feature, you can configure Cisco netManager to send reports to e-mail addresses at regularly scheduled intervals.

Configuring Recurring Reports

To create a new Recurring Report:

Step 1 From the Cisco netManager console, select **Configure > Recurring Reports.**

Step 2 On the Recurring Reports dialog, click **New** to create a new report.

Step 3 On the General dialog, enter a title for the report in the Report name box.

Step 4 Enter the full URL path to the report.

You can find this path by selecting a report in the web interface. The URL shown in the address bar is the URL you will want to enter in the URL box.

Step 5 Click **Next**.

Step 6 On the Schedule dialog, select the date and time on which to send the report.

Step 7 Click **Next**.

Step 8 On the E-mail dialog, enter the e-mail (SMTP) information for the e-mail address to which you are sending the report.

- **E-mail address**—Enter an e-mail address to which you would like the report sent.
- **Outgoing mail (SMTP) server**—Enter the SMTP server for your network.
- **Port**—Enter the port number for the mail server.
- **From**—Enter an e-mail address for the sender. The default address is taken from Cisco netManager.
- **Subject**—Enter a subject for the report e-mail.
- **Send reports as attachments**—Select this option to have reports sent as attachments, rather than as inline text within the original e-mail. Workspace reports can only be sent as attachments.

Note The e-mail contains a report link that promptst you to log in to the Cisco netManager homepage if you are not already logged in. To go directly to the report, open the e-mail again and click the link.

Step 9 Click **Finish** to add the report.

To edit an existing Recurring Report:

Step 1 From the From the Cisco netManager console, select **Configure > Recurring Reports.**

Step 2 On the Recurring Reports dialog, select an existing Recurring Report and click **Edit**.

Step 3 Complete the Recurring Report dialogs as you would for creating a new Recurring Report.

Testing Recurring Reports

To test a recurring report before the scheduled time and date:

Step 1 From the Cisco netManager console, select **Configure** > **Recurring Reports**.

Step 2 On the Recurring Reports dialog, select a report and click **Test.**

Step 3 After the test is complete, a popup message tells you whether the test was successful.