User Guide for Cisco netManager 1.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

OL-17035-01

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for Cisco netManager 1.1

CONTENTS

Audience xiii

Conventions xiii

Important Information About Product Configurations xiv

Product Documentation xiv

Obtaining Documentation, Obtaining Support, and Security Guidelines xv

CHAPTER 1 **Cisco netManager Overview** 1

Starting Cisco netManager 2

Step 1: Launch the Web Interface 2

Step 2: Discover Devices 3

Step 3: View Network Data 3

Step 4: Set Up Actions 4

Cisco netManager Web Interface 4

Using the GO Menu 4

Cisco netManager Tabs 6

Home Tab 7

Devices Tab 7

Reports Tab 7

Device Management 8

Workspaces 8

Topology Views 9

Polling and Listening 10

Actions 10

CHAPTER 2 **Managing Devices** 1

Device Services 1

About the Devices Tab 2

Device List 2

Context-Sensitive Menu 3

Device Toolbar 4

Device States and Icons 4

Adding a New Device 4

- Active/Performance Monitors Scan Properties 5

Using the Device Discovery Wizard 6

- Device Discovery Scan Types 7
- Device Discovery Example 7
- About IP Phone Discovery 9

Importing Devices from a File 9

- Sample CSV Files 10

Configuring Network Interfaces on a Device 12

Configuring Credentials 12

Editing SNMP Timeout and Retries 12

Adding Attributes to a Device 13

Adding Notes to a Device 13

Changing a Device IP Address 14

Changing a Device Name 14

Rediscovering Devices 14

Suspending and Resuming Single Device Polling 14

Understanding Device Groups 15

- Working with System-Defined Groups 15
  - Creating a Device Group 16
  - Modifying Group Properties 16
  - Creating a User-Defined Group 17
  - Modifying Group Access Rights for a User 17
  - Renaming a Device Group 17
- Using Dynamic Groups 17
  - Creating Dynamic Groups 18
  - Dynamic Group Examples 19
- Creating Access Rights for a Device Group 23
  - User Access Rights for a Device Group 24

Understanding Device Properties 24

- General Device Properties 25
- Device Property Performance Monitors 26
- Active Monitor Device Properties 29
- Passive Monitor Device Properties 29
- Device Property Actions 29
- Device Property Credentials 30
- Device Property Polling 30
- Device Property Notes 31
- Device Property Custom Links 31

Device Property Attributes 31
Changing Device Types 32
Editing Multiple Devices with Bulk Field Change 32
Using Acknowledgements 33

CHAPTER 3

Understanding Workspaces and Workspace Content 1
About Workspaces 1
Home Workspace 1
Home Page View 2
Problem Areas 1 and Problem Areas 2 2
Device Status Workspace 2
Workspace Toolbar 3
Managing Workspace Views 4
Creating a New Workspace View 5
Editing a Workspace View 5
Deleting a Workspace View 6
Navigating Through Workspaces 7
Workspace Toolbar 7
About Workspace Content 7
Workspace Content Categories 8
Workspace Content Types 9
CPU Utilization Workspace Content 9
Custom Performance Monitor Workspace Content 10
Device Workspace Content 11
Disk Utilization Workspace Content 12
General Workspace Content 13
Interface Utilization Workspace Content 13
Inventory Workspace Content 14
Memory Utilization Workspace Content 15
Performance - Historic Workspace Content 16
Performance - Last Poll Workspace Content 16
Ping Availability and Response Time Workspace Content 17
Problem Areas Workspace Content 18
Threshold Workspace Content 19
Top 10 Workspace Content 20
About the Workspace Content Menu 21
Configuring Workspace Content 21
Moving Workspace Content Within a Workspace 21

CHAPTER 4

Using Topology Views 1

Using the Service Level View 1

Starting the Service Level View 2

Understanding the Layout of the Service Level View 2

Phones Pane 3

Using the Search Tool to Locate a Phone 3

Launching a Phone Report from the Service Level View 3

Map Display Pane 4

Using the Physical Connectivity View 5

Understanding the Layout of the Physical Connectivity View 6

Starting the Physical Connectivity View 7

Displaying IP Address or Display Name 7

Topology Views Legend 7

Launching Cisco netManager Tools 11

Viewing Events Information 12

Acknowledging All Device Events 12

Viewing Device Information 12

Viewing Phones Report 12

Launching Administration Pages for Devices 13

Connecting to the Device Using Web Launch 13

Launching Network Tools 13

Using the Ping Tool 14

Using the DNS Lookup Tool 14

Using the Trace Route Tool 14

Using the Telnet Tool 15

Using the MAC Address Tool 15

CHAPTER 5

Polling 1

Changing How You Poll Devices 1

Using Maintenance Mode 2

Setting the Polling Interval 2

Stopping and Starting Polling 2

Stopping and Starting Polling On a Monitor 2

Dependencies Overview 3

Setting Dependencies 3

Viewing Dependencies 4

IPX Support 4

CHAPTER 6 **Using Actions** 1

About Action Strategies 2

About the Action Library 2

Configuring an Action 3

Action Builder Wizard 4

Creating a Beeper Action 4

Port Settings 5

Creating a Pager Action 6

Creating an E-Mail Action 6

Creating an SMS Action 7

Creating a Sound Action 8

Creating a WinPopup Action 9

Creating a Syslog Action 9

Creating a Text-to-Speech Action 10

Creating a Program Action 10

Creating an Active Script Action 11

Creating a Web Alarm Action 12

Dismissing or Muting Web Alarms 12

Creating a Service Restart Action 13

Configuring Recurring Actions 14

Testing an Action 15

Deleting an Action 15

Assigning an Action to a Device 15

Assigning an Action to a Monitor 16

Creating a Blackout Period 17

About Percent Variables 18

About Action Policies 21

Creating an Action Policy 21

Editing Action Policies 22

Implicit Action Policy 22

About Acknowledgements 23

Example: Getting an E-Mail Alert when the Web Server Fails 23

CHAPTER 7 **Using Notifications** 1

Notification Filtering 1

What Are Notification Criteria? 2

Limiting Notifications to Those for Specific Events 2

Configuring Notifications 2

Adding and Editing Device Notification Rules 3
Cloning a Notification Rule 4
Viewing Notification Rule Configuration Details 5
Deleting Notification Rules 5

CHAPTER 8 **Using Active Monitors 1**
About Monitors and Actions 1
Using Monitors and Actions 1
About the Active Monitor Library 2
Supported Active Monitor Types 2
Assigning Active Monitors 3
Deleting Active Monitors 4
Using the Bulk Field Change Feature 5
Group and Device Active Monitor Reports 5
Example: Monitoring Network Printer Toner Levels 5
Expression Editor 6
Script Syntax 6
Keywords 7
Regular Expression Syntax 11
Text String Example 13
Using Telnet to Determine "Expect on Connect" String 14
Using Active Script Monitor 14
Examples: Active Script Monitor Context Code 15
Using the Active Script Monitor Context Object 21
Properties 23
Properties Example1 1 23
Properties Example 2 24

CHAPTER 9 **Using Passive Monitors 1**
Passive Monitors Icon 1
Configuring Passive Monitor Listeners 1
Using the Passive Monitor Library 2
Adding or Editing Passive Monitors 2
Assigning a Passive Monitor to a Device 3
Accessing Group and Device Passive Monitor Reports 3
Receiving SNMP Traps 3

CHAPTER 10 **Using Performance Monitors** 1

Understanding the Performance Monitor Library 2

Enabling SNMP on Windows Devices 2

Configuring and Enabling Performance Monitors 3

Adding Custom Performance Monitors to the Performance Monitor Library 6

Configuring an SNMP Monitor 7

Configuring a WMI Monitor 7

Configuring an SNMP Active Script Performance Monitor 8

Configuring a WMI Active Script Performance Monitor 9

Performance Reporting 9

Example: Monitoring Router Bandwidth 12

Configuring the Monitor 13

Viewing the Data 13

Example: Troubleshooting a Slow Network Connection 14

CHAPTER 11 **Using Reports** 1

Report Categories 1

Selecting a Report 2

About Data Collection for Reports 2

Changing the Number of Records Displayed 2

About System Reports 3

About Group Reports 3

About Device Reports 3

About Phone Reports 4

List of Reports 5

Active Discovery Log 9

Active Monitor Availability 9

Active Monitor Availability per Device 9

Action Log 10

Actions Applied 10

Active Monitor Outage 10

Activity Log 11

All IP Phones/Lines 11

Chassis Inventory Details 11

CPU Utilization per Group 12

CPU Utilization per Device 12

Custom Performance Monitors 12

Device Status 13

Devices Import Status 13
Devices Reports 14
Disk Utilization per Group 14
Disk Utilization per Device 15
Event History 15
Events 16
Flash Devices Inventory 16
Flash Files Inventory 16
Fan Status 17
General Error Log 17
Health 17
Health per Device 18
Home Workspace 18
Interface Details 18
Interface Utilization per Group 19
Interface Utilization per Device 20
IP Phone Audit 21
IP Phone Audit Report per Device 22
IP Phone Audit Report per Group 22
IP Phone Move 23
IP Phone Move Report per Device 23
IP Phone Move Report per Group 24
IP Phones and Lines per Device 24
IP Phones and Lines per Group 25
Memory Utilization per Group 25
Memory Utilization per Device 26
Module Inventory 26
Passive Monitor Error Log 27
Performance Monitor Error Log 27
Ping Availability 28
Ping Availability per Device 28
Ping Response Time 29
Ping Response Time per Device 29
Power Supply Status 29
Recurring Action Log 29
Recurring Report Log 30
Registered Phones Report 30
SNMP Trap Log 31
SNMP Trap Log per Device 31
Stack Inventory 31

State Change Acknowledgement 32
State Change Timeline per Group 32
State Change Timeline per Device 32
State Summary 33
Syslog Entries 33
Syslog Entries per Device 33
Temperature Statistics 34
Top 10 34
Cisco Unity Port Details 34
Cisco Unity Port Utilization 35
Unregistered IP Phones 35
Voice Gateway Details 35
Voice Services Details 36
Web User Activity Log 36
Windows Event Log 36
Windows Event Log per Device 36
Wireless LWAP Summary 37
Wireless LWAP Channel Utilization 37
Printing, Exporting, and Saving Reports 38
Date/Time Drop-Down List 39
Zoom Tool 39
Adding a Report to Your List of Favorites 39
Using Recurring Reports 40
Configuring Recurring Reports 40
Testing Recurring Reports 41

CHAPTER 12 **Using SNMP** 1
Monitoring SNMP Service 1
Assigning SNMP Active Monitor to a Device 1
About the SNMP Agent or Manager 2
About the SNMP MIB 2
About SNMP Object Names and Identifiers 3
About SNMP Operations 3
About SNMP Security 3
Using the Trap Definition Import Tool 4
Configuring Global SNMP Timeout and Retry Settings 4

CHAPTER 13 **Administrative Tasks** 1

About Web Security 1

Configuring IP Security 1

Stopping and Starting the Web Server 2

Configuring the Web Server 2

Configuring the Web Interface to use IIS 2

Resolving IIS Scanning-Device Error 4

Configuring LDAP 4

Managing Users 5

Changing Admin Preferences (Password Change) 7

Using the Cisco netManager Console 7

Changing the Date and Time Format 7

Changing How Long Report Data Is Stored 8

Changing the Device State Colors or Icons 8

Changing Clock or Regional Preferences 8

Managing Notifications 9

Configuring SMTP Load 9

Performance and E-Mail Details 9

Configuring Socket Timeouts 10

Notification Logging 10

APPENDIX A **Events Processed** 1

Lists of Events 1

APPENDIX B **Processed SNMP Traps and Corresponding Cisco netManager Events** 1

Processed Standard SNMP Traps (RFC 1215) 1

Processed CISCO-UNITY-EXPRESS-MIB Traps 1

Processed CISCO-CCME-MIB Traps 2

Processed CISCO-SRST-MIB Traps 2

APPENDIX C **Open Source License Acknowledgements** 1

Notices 1

OpenSSL/Open SSL Project 1

INDEX

Preface

This manual describes Cisco netManager and provides instructions for using and administering it.

Audience

The audience for this document includes:

- Administrators who monitor the status of the device network.
- Users who verify operational status using topology displays, search for phone and device information, and view and act on operational alerts on devices and phones in the network.

Note Administrators have access to all the features in Cisco netManager. Administrators can assign different access privileges to any user. All other users, by default, have read-only privileges and can only view information.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option>Network Preferences**
Selecting a menu item in tables	Option>Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Important Information About Product Configurations

Cisco netManager is available in two product configurations: Cisco netManager IP Infrastructure and Cisco netManager Unified Communications. Cisco netManager IP Infrastructure provides standards-based monitoring of network devices, services, or applications on TCP/IP and Windows. Cisco netManager Unified Communications includes all features of Cisco netManager along with the additional capability to provide visibility into, and monitoring of, Cisco Unified Communications devices. See the *Quick Start Guide for Cisco netManager* for licensing information.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

The Cisco netManager 1.1 documentation set applies to both Cisco netManager IP Infrastructure and Cisco netManager Unified Communications. Within each document are notes about whether a feature applies only to Cisco netManager Unified Communications.

The following table lists the Cisco netManager Unified Communications 1.1 locations on Cisco.com.

Table 1 Product Documentation

Document Title	Available Formats
Supported Devices Table for Cisco netManager 1.1	On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps7243/products_device_support_tables_list.html
Release Notes for Cisco netManager 1.1	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps7243/prod_release_notes_list.html

Table 1 Product Documentation (continued)

Document Title	Available Formats
Quick Start Guide for Cisco netManager 1.1	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps7243/prod_installation_guides_list.html
User Guide for Cisco netManager 1.1	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps7243/products_user_guide_list.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Cisco netManager Overview

Cisco netManager is a network monitoring solution that allows you to visualize,diagnose and report status of your data and Unified Communications deployment. It monitors all components of the network to provide real-time operational status so you can identify network failures before they become catastrophic.

Cisco netManager is available in two product configurations: Cisco netManager IP Infrastructure and Cisco netManager Unified Communications. Cisco netManager IP Infrastructure provides standards-based monitoring of network devices, services, or applications on TCP/IP and Windows. Cisco netManager Unified Communications includes all features of Cisco netManager along with the additional capability to provide visibility into, and monitoring of, Cisco Unified Communications devices.

Note The ability to view and monitor Cisco Unified Communications Manager depends upon the type of licensing you have. Please see the *Quick Start Guide for Cisco netManager 1.1* for licensing information.

Cisco netManager includes the following key features:

- A web interface that provides customizable workspaces and multiuser support to monitor operational status of all supported network and office devices.
- Automated discovery of network elements. Information gathered include detailed inventory and device capability information. Cisco netManager also has the capability to import devices into the system via bulk import or a single device at a time.
- Service-level and physical topology views of network devices that display current operational, performance, and device application status. This allows for faster trouble isolation through diagnostic tools with access to embedded device management tools.
- Real-time operational and performance monitoring with system-defined thresholds and events.
- Notification services: E-mail, Short Message Service (SMS), and Simple Network Management Protocol (SNMP) traps.
- Basic diagnostics capabilities including ping, traceroute, Telnet, and Domain Name System (DNS) lookup.
- A wide variety of real-time and historical reports that provide performance and availability information related to the devices in your network. Report types include the following:
  - Performance reports: Performance data for a selected device or device group
  - Problem areas: Alerts reported across the network and across different data sources; for example, traps, syslogs, event logs, and performance errors.

- Event history: Historical reports of all events generated by Cisco netManager for a given device or device group.
- General: Reports on application logs, user activity, and so on.

Table 1-1 includes common tasks and corresponding sections in the online help and user guide that pertain to those tasks:

Table 1-1 Cisco netManager Common Tasks

Task	Section
View service-level and physical topologies of network devices that display current operational, performance, and device application status.	Chapter 4, "Using Topology Views"
Monitor performance (CPU, disk, memory, and interface use) for critical devices.	Device List, page 2-2 Chapter 4, "Using Topology Views"
Monitor standard IP services , such as HTTP, FTP, or SMTP on a device.	Chapter 8, "Using Active Monitors"
Set up workspace views for your users.	Chapter 3, "Understanding Workspaces and Workspace Content"
Set up users and role-based security access.	Managing Users, page 13-5
Set up and route alerts to the appropriate network administrator.	Chapter 6, "Using Actions" Chapter 7, "Using Notifications"
View full reports to troubleshoot and monitor performance and historical data.	Chapter 11, "Using Reports"
Group devices by type, location, services, or some other attribute.	Using Dynamic Groups, page 2-17

Starting Cisco netManager

To quickly start Cisco netManager, you should do the following:

1. Launch the Web Interface, page 1-2
2. Discover Devices, page 1-3
3. View Network Data, page 1-3
4. Set Up Actions, page 1-4

Step 1: Launch the Web Interface

You can connect to the Cisco netManager web interface from any browser by entering its web address. This web address consists of the hostname of the Cisco netManager host and the web server port number. The default port number is 80.

For example, if your Cisco netManager host is named monitor1.cisco.com, then the web address will be http://monitor1.cisco.com:80.

Note When you use the default port number (80), you do not have to include the port number in the address.

There are two default users on the web server:

- Administrator (Username: `admin` Password: `admin`)
- Guest (Username: `guest` Password: `<password box left blank>`

For more information about user privileges, see Managing Users, page 13-5.

To change the default administrator password:

Step 1 From the web interface, click **GO** > **Configure** > **Preferences...**.

Step 2 Click **Change your password**.

Step 2: Discover Devices

There are several ways to add devices to Cisco netManager. See the following sections for more information:

- Adding a New Device—Manually adds a device using its IP address or hostname.
- Using the Device Discovery Wizard—Automatically detects network devices (workstations, servers, routers, hubs, and so on), scans those devices for services, and lets you select the devices that you want to manage. The Device Discovery Wizard is only available from the Cisco netManager console. The console is only available from the server where Cisco netManager is installed (**Start > All Programs > Cisco netManager 1.1 > Cisco netManager 1.1 Discovery**).
- Importing Devices from a File—Imports multiple devices using a seed file.

Step 3: View Network Data

Begin viewing your network using the following tools:

- Topology Views
  - Service Level View displays a logical topology view of your Cisco Unified Communications network.

    Note The Service Level View is available only if you have purchased a license that monitors Unified Communication devices.

  - Physical Connectivity View gives you a visual representation of all physical devices and connections in your network. This view gives a quick snapshot of your entire network including its overall health.
- Workspaces—Contain multiple *views* that let you organize workspace content by the type of information they display.
- Reports—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.

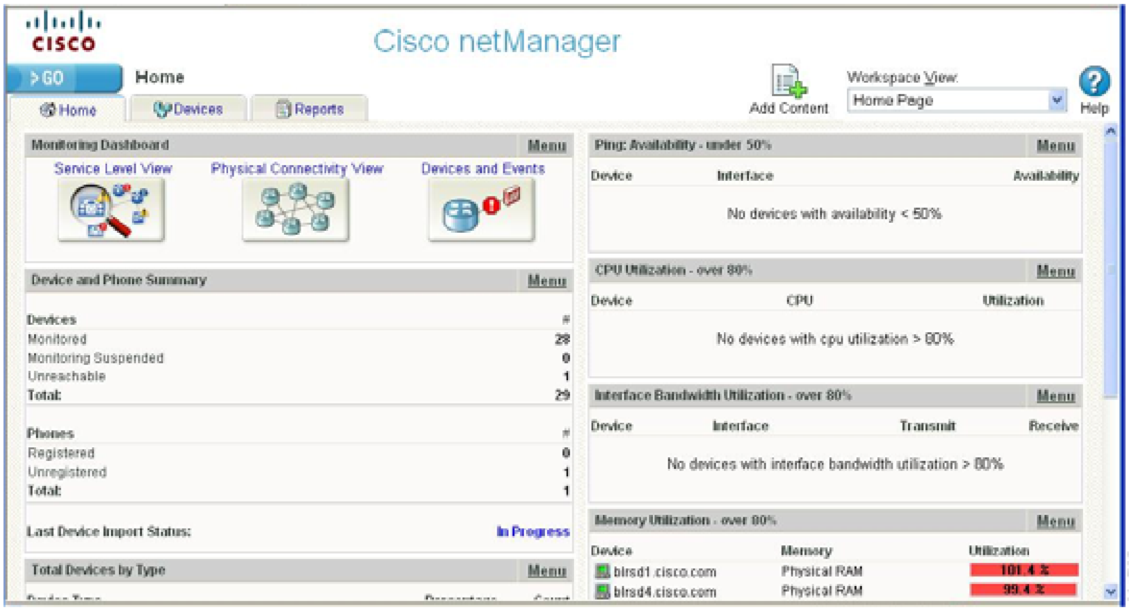
Step 4: Set Up Actions

After selecting devices, configure actions that will notify you when changes occur on the monitored devices. For more information, see Using Actions.

After you have completed discovery and set up basic monitoring of devices and services, you can investigate the other features of Cisco netManager. The following sections contain information on navigating the web interface and the various tools available to you.

Cisco netManager Web Interface

The Cisco netManager HomeSpace workspace is the first screen you see after logging in to the web interface. For more information on your home workspace, see About Workspaces, page 3-1.



Workspace View: Home Page

Device and Phone Summary

Devices	#
Monitored	28
Monitoring Suspended	0
Unreachable	1
Total:	29

Phones	#
Registered	0
Unregistered	1
Total:	1

Last Device Import Status: In Progress

Total Devices by Type

Ping: Availability - under 50%

Device	Interface	Availability

No devices with availability < 50%

CPU Utilization - over 80%

Device	CPU	Utilization

No devices with cpu utilization > 80%

Interface Bandwidth Utilization - over 80%

Device	Interface	Transmit	Receive

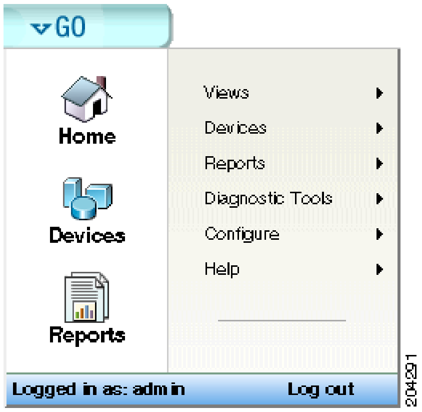
No devices with interface bandwidth utilization > 80%

Memory Utilization - over 80%

Device	Memory	Utilization
blrsd1.cisco.com	Physical RAM	101.4 %
blrsd4.cisco.com	Physical RAM	99.4 %

Using the GO Menu

The main menu for the web interface is housed within the GO button, located in the upper-left corner of your browser. The GO menu is visible from anywhere within the web interface.



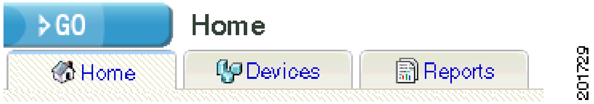
From the **GO** menu, you can navigate to the areas you will use most in Cisco netManager, including your Home workspace views; your monitored devices list; diagnostic tools; and the configuration of the Passive, Active, and Performance Monitor libraries. Table 1-2 lists tasks available through the GO menu and provides corresponding sections in this document, to help you.

Table 1-2 GO Menu Options

Category	Operation	Section/Description
Views	Physical Connectivity View	Using the Physical Connectivity View, page 4-5
	Service Level View	Using the Service Level View, page 4-1
Devices	My Network	About the Devices Tab, page 2-2
	New Device	Adding a New Device, page 2-4
	Import Devices	Importing Devices from a File, page 2-9
	Rediscover Devices	Rediscovering Devices, page 2-14
	New From Active Discovery Results	Using the Device Discovery Wizard, page 2-6
	Web Alarms	Dismissing or Muting Web Alarms, page 6-12
Reports	Overview	Report Categories, page 11-1
	All Reports	Selecting a Report, page 11-2
	System	About System Reports, page 11-3
	Group	About Group Reports, page 11-3
	Device	About Device Reports, page 11-3
	Performance	Report Categories, page 11-1
	Problem Areas	
	General	
	Favorites	
Diagnostic Tools	Ping	Using the Ping Tool, page 4-14
	Traceroute	Using the Trace Route Tool, page 4-14
	DNS Lookup	Using the DNS Lookup Tool, page 4-14
	MAC Address	Using the MAC Address Tool, page 4-15

Category	Operation	Section/Description
Configure	Performance Monitor Library	Understanding the Performance Monitor Library, page 10-2
	Active Monitor Library	About Monitors and Actions, page 8-1
	Passive Monitor Library	Configuring Passive Monitor Listeners, page 9-1.
	Action Library	About the Action Library, page 6-2
	Action Policies	About Action Policies, page 6-21
	Credentials Library	Credentials, page 2-6
	Recurring Actions	Configuring Recurring Actions, page 6-14
	Threshold Settings	Configuring Threshold Settings, page 3-20
	Physical Connectivity View Settings	Displaying IP Address or Display Name, page 4-7
	Notification Settings	Configuring Notifications, page 7-2
	Default SNMP Timeout	Configuring Global SNMP Timeout and Retry Settings, page 12-4
	Manage Web Server	Configuring the Web Server, page 13-2
	Manage Users	Managing Users, page 13-5
	Manage Workspace Views	Managing Workspace Views, page 3-4
	LDAP Credentials	Configuring LDAP, page 13-4
	IP Security	Configuring IP Security, page 13-1
	Preferences	Changing Admin Preferences (Password Change), page 13-7
	Report Preferences	Changing the Number of Records Displayed, page 11-2

Cisco netManager Tabs



The web interface is organized into three tabs:

- Home
- Devices
- Reports

You can access each of these areas by:

- Clicking on an icon from the **GO** menu.
- Selecting one of the web interface tabs.

Home Tab

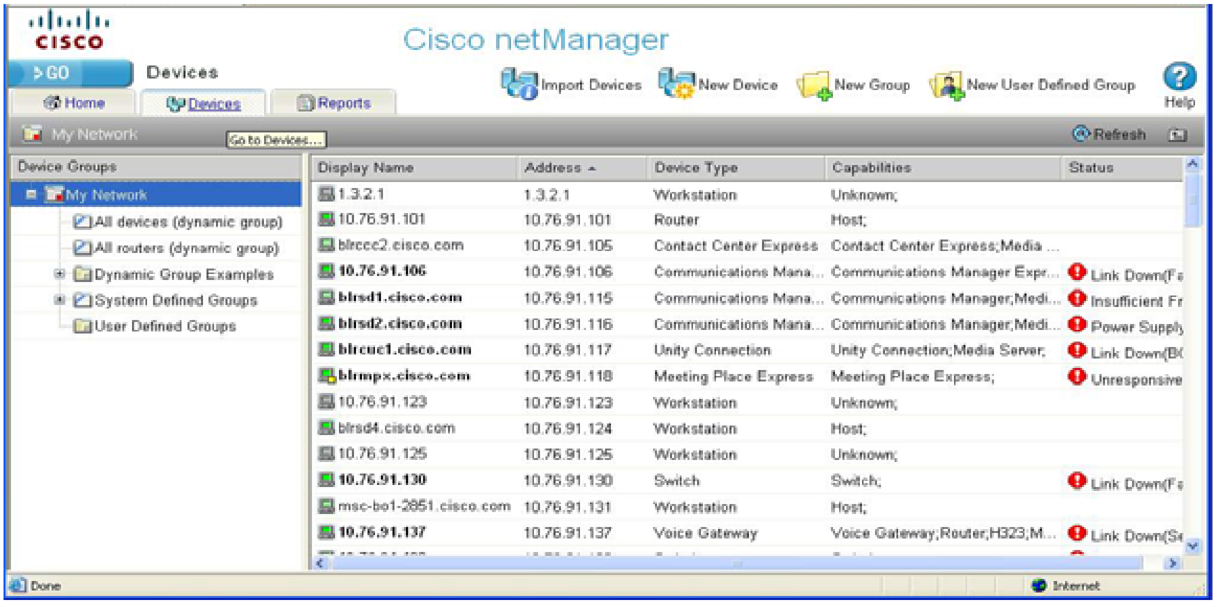
This universal workspace is designed to house the network information that you typically need. The default Home workspace view cannot be customized, but you can make a copy of it and then add different types of workspace content. This customizable view allows you to focus on certain network element information that is of importance. For more information on the Home workspace and workspace content, see Chapter 3, "Understanding Workspaces and Workspace Content."

Devices Tab

The Devices tab is where you can manage and display monitored devices. For more information, see Chapter 2, "Managing Devices."

Figure 1-1 shows an example of the Devices page.

Figure 1-1 *Devices Page*



Display Name	Address ▲	Device Type	Capabilities	Status
1.3.2.1	1.3.2.1	Workstation	Unknown;	
10.76.91.101	10.76.91.101	Router	Host;	
blrccc2.cisco.com	10.76.91.105	Contact Center Express	Contact Center Express;Media ...	
10.76.91.106	10.76.91.106	Communications Mana...	Communications Manager Expr...	Link Down(F
blrsd1.cisco.com	10.76.91.115	Communications Mana...	Communications Manager;Medi...	Insufficient Fr
blrsd2.cisco.com	10.76.91.116	Communications Mana...	Communications Manager;Medi...	Power Supply
blrcuc1.cisco.com	10.76.91.117	Unity Connection	Unity Connection;Media Server;	Link Down(B(
blrmpx.cisco.com	10.76.91.118	Meeting Place Express	Meeting Place Express;	Unresponsive
10.76.91.123	10.76.91.123	Workstation	Unknown;	
blrsd4.cisco.com	10.76.91.124	Workstation	Host;	
10.76.91.125	10.76.91.125	Workstation	Unknown;	
10.76.91.130	10.76.91.130	Switch	Switch;	Link Down(F
msc-bo1-2851.cisco.com	10.76.91.131	Workstation	Host;	
10.76.91.137	10.76.91.137	Voice Gateway	Voice Gateway;Router;H323;M...	Link Down(S

Reports Tab

The Reports tab opens the Reports page, which contains all of the Cisco netManager reports. Reports provide current status, performance, and historical data for devices and monitors. Workspaces let you focus on segments of the network and create your own views into the report data. They provide crucial network data in one location, which allows for quick and easy access. Cisco netManager offers over 100 instances of workspace content and reports. Each administrative user can have their own workspace with configurable workspace content. Once configured, these reports can help you troubleshoot problem areas on your network and allow easy access to important network information.

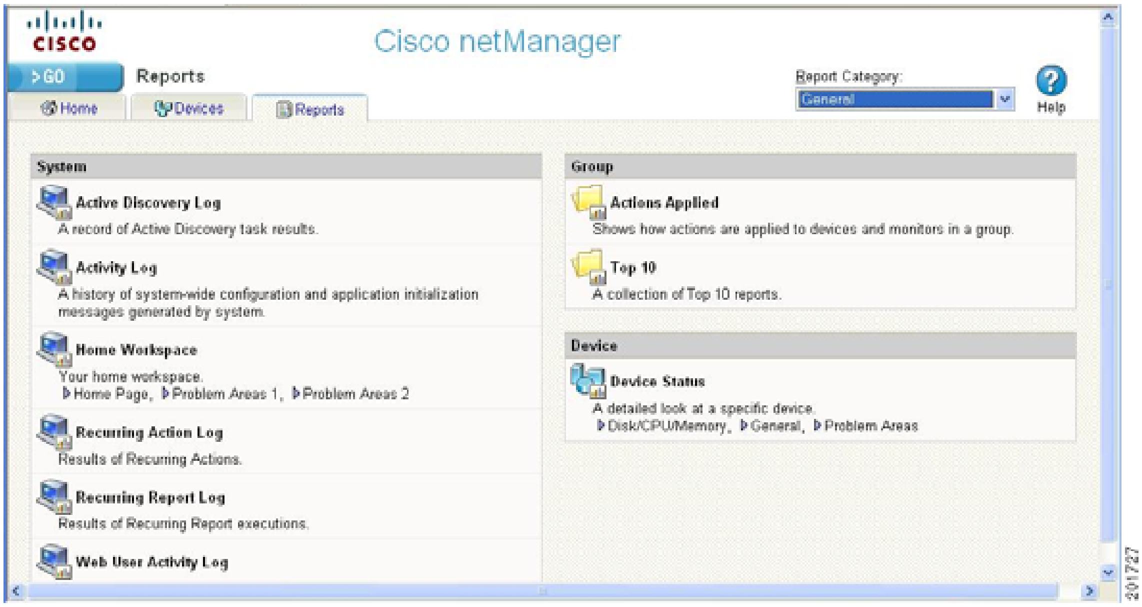
For more information on reports and workspaces, see the following:

- Chapter 11, "Using Reports"
- Chapter 3, "Understanding Workspaces and Workspace Content"

Reports can be sent on a regular basis to an e-mail address you identify through the Recurring Report feature. Reports configured and viewed from the Reports tab are fully functioning reports. Miniature versions of these reports, or workspace content, are available for display purposes only in a workspace.

Figure 1-2 shows an example of the General Reports page.

Figure 1-2 General Reports Page



System

Active Discovery Log
A record of Active Discovery task results.

Activity Log
A history of system-wide configuration and application initialization messages generated by system.

Home Workspace
Your home workspace.
Home Page, Problem Areas 1, Problem Areas 2

Recurring Action Log
Results of Recurring Actions.

Recurring Report Log
Results of Recurring Report executions.

Web User Activity Log

Group

Actions Applied
Shows how actions are applied to devices and monitors in a group.

Top 10
A collection of Top 10 reports.

Device

Device Status
A detailed look at a specific device.
Disk/CPU/Memory, General, Problem Areas

Report Category Menu

The Report Category menu allows you to jump to different report categories.

Device Management

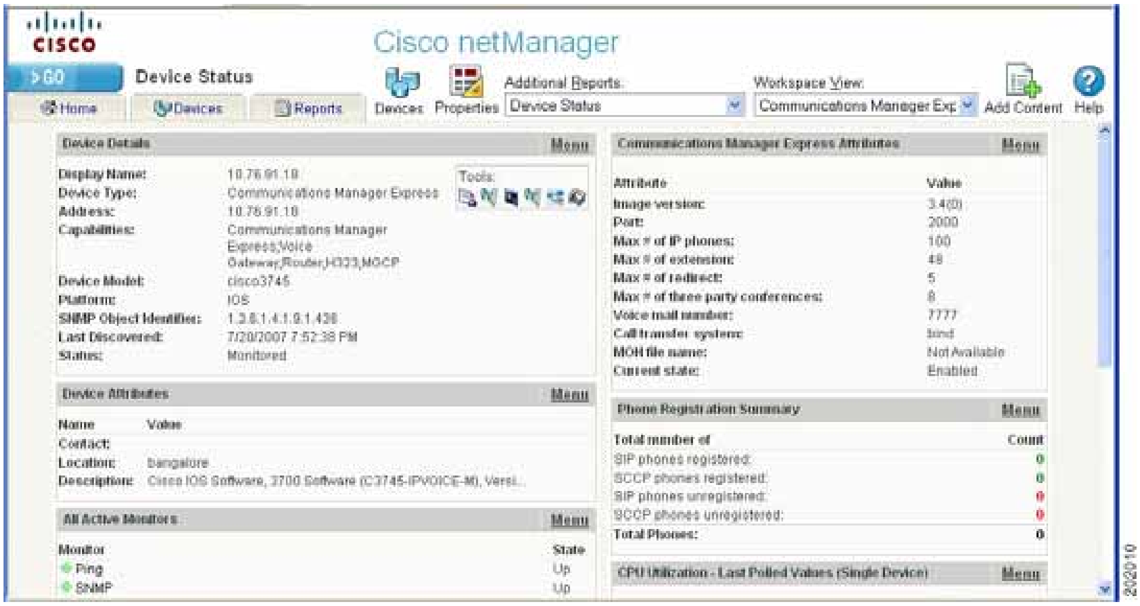
After installing Cisco netManager you can import device credentials using a seed file or add individual devices manually or as a map. The device list shows a summary of all monitored devices in your network and also allows you to perform various tasks using the context menu. For more information, see Chapter 2, "Managing Devices."

Workspaces

Workspaces are designed to house network and device information that you typically need to view. There are two types of workspaces: Home and Device Status. Home workspace contains various network information and Device Status workspace displays device-level information. Workspaces contain multiple *views* that let you organize workspace content by the type of information they display. When you begin customizing your workspace views, you should consider the types of information you need to view most often, the devices to which you need to pay closest attention, and the level of detail you want to monitor through a particular workspace view. You should also take into consideration the type of workspace, and the types of workspace content you can add. For more information on workspaces and workspace content, see Chapter 3, "Understanding Workspaces and Workspace Content."

Figure 1-3 shows an example of a Device Status workspace.

Figure 1-3 Device Status Workspace



Device Details

Display Name:	10.76.91.10
Device Type:	Communications Manager Express
Address:	10.76.91.10
Capabilities:	Communications Manager Express,Voice Gateway,Router,H323,MGCP
Device Model:	cisco3745
Platform:	IOS
SNMP Object Identifier:	1.3.6.1.4.1.9.1.438
Last Discovered:	7/20/2007 7:52:38 PM
Status:	Monitored

Device Attributes

Name	Value
Contact:	
Location:	bangalore
Description:	Cisco IOS Software, 3700 Software (C3745-IPVOICE-M), Versi...

All Active Monitors

Monitor	State
Ping	Up
SNMP	Up

Communications Manager Express Attributes

Attribute	Value
Image version:	3.4(0)
Port:	2000
Max # of IP phones:	100
Max # of extension:	48
Max # of redirect:	5
Max # of three party conferences:	8
Voice mail number:	7777
Call transfer system:	blind
MOH file name:	Not Available
Current state:	Enabled

Phone Registration Summary

Total number of	Count
SIP phones registered:	0
SCCP phones registered:	0
SIP phones unregistered:	0
SCCP phones unregistered:	0
Total Phones:	0

CPU Utilization - Last Polled Values (Single Device)

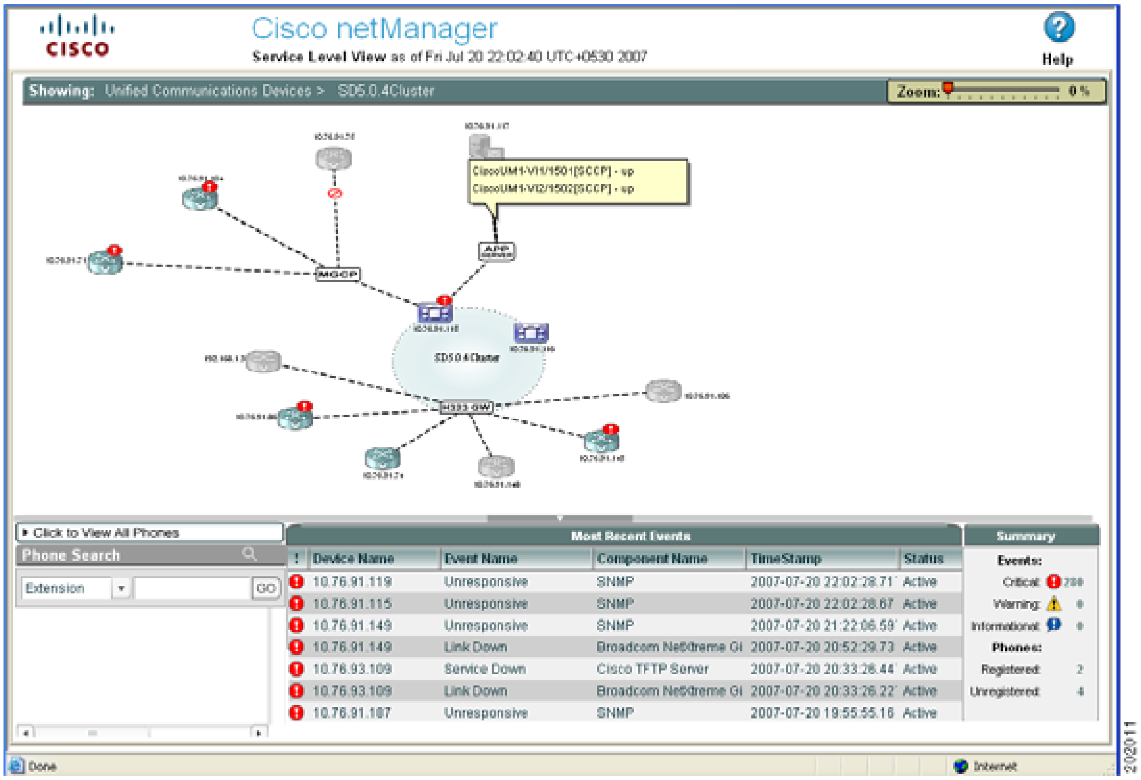
Topology Views

Cisco netManager provides two topological views of your network:

- Service Level View displays a logical topology view of Unified Communication devices in your network.
- Topology View displays a physical topology view of all the physical connections and devices in your network.

For more information, see Chapter 4, “Using Topology Views.” Figure 1-4 shows an example of a Service Level View.

Figure 1-4 Service Level View



Service Level View as of Fri Jul 20 22:02:40 UTC+0530 2007

Showing: Unified Communications Devices > SD5.0.4Cluster

CiscoUM1-VI1/1501[SCCP] - up
CiscoUM1-VI2/1502[SCCP] - up

!	Device Name	Event Name	Component Name	TimeStamp	Status
●	10.76.91.119	Unresponsive	SNMP	2007-07-20 22:02:28.71	Active
●	10.76.91.115	Unresponsive	SNMP	2007-07-20 22:02:28.67	Active
●	10.76.91.149	Unresponsive	SNMP	2007-07-20 21:22:06.59	Active
●	10.76.91.149	Link Down	Broadcom NetXtreme Gi	2007-07-20 20:52:29.73	Active
●	10.76.93.109	Service Down	Cisco TFTP Server	2007-07-20 20:33:26.44	Active
●	10.76.93.109	Link Down	Broadcom NetXtreme Gi	2007-07-20 20:33:26.22	Active
●	10.76.91.107	Unresponsive	SNMP	2007-07-20 19:55:55.16	Active

Events:
Critical: 200
Warning: 0
Informational: 0
Phones:
Registered: 2
Unregistered: 4

Polling and Listening

Cisco netManager actively polls devices to determine their status. You can use preconfigured monitors, or create your own, to poll services on a device, and to passively listen for messages sent across the network. Monitors can also report on device performance by checking and reporting on device resources, such as disk, CPU, and interfaces. For more information on polling and monitors see the following:

- Chapter 5, "Polling"
- Chapter 8, "Using Active Monitors"
- Chapter 9, "Using Passive Monitors"

Actions

Depending on the responses received from polling, or the types of messages received, Cisco netManager initiates actions to notify you of any change on your network. Actions speed problem resolution through options such as alerting via e-mail or pager, or restarting a service. For more information on actions, see Chapter 6, "Using Actions."

CHAPTER 2

Managing Devices

Before Cisco netManager can monitor devices, you need to add devices. To add devices to Cisco netManager, see one of the following:

- Adding a New Device, page 2-4
- Using the Device Discovery Wizard, page 2-6
- Importing Devices from a File, page 2-9

Devices are organized through device groups. By default, all of the devices on your network are placed into a Dynamic Group named All devices. For more information on device groups, see Understanding Device Groups, page 2-15.

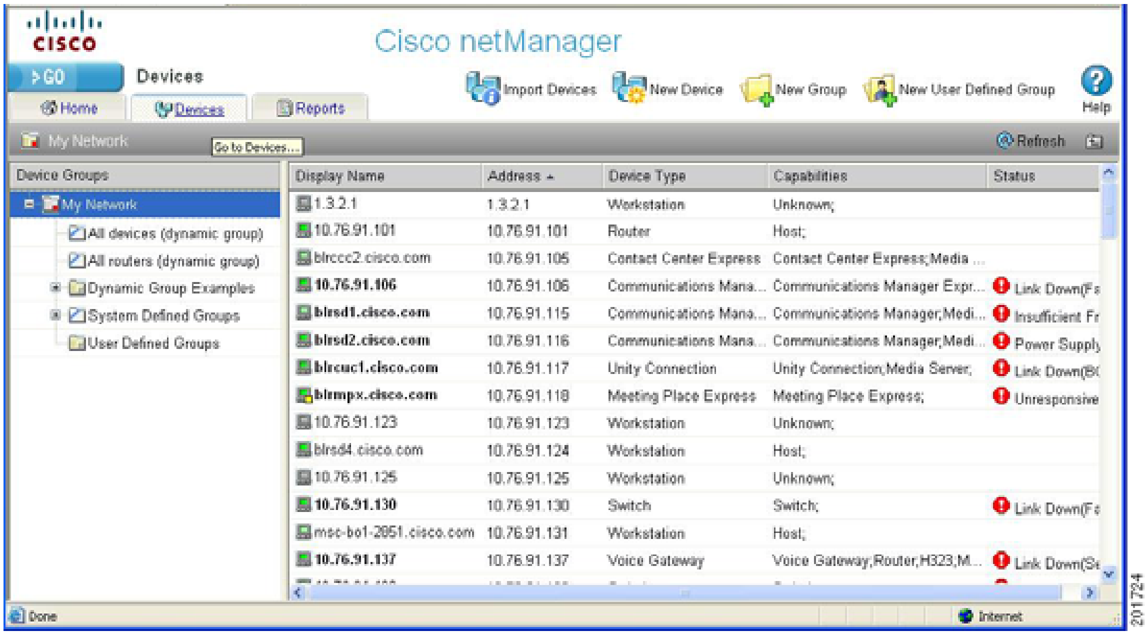
Device Services

Cisco netManager associates active monitors with devices on your network. Active monitors query the network services active on a device and then wait for a response. These monitors query the services running on a network resource, checking to make sure that the FTP server, web server, e-mail server, etc., are up and responding. Active monitors include DNS, SNMP, Telnet, Ping, TCPIP, and NT Service. If a response is either not received or is not what is expected, the service is considered down. If the query is returned as expected, the service is considered up. If any one service on a device is down, then the device as a whole is considered down.

For a more information about service monitors, see Chapter 8, “Using Active Monitors.”

About the Devices Tab

This view provides an overview of all the devices in your network.



Display Name	Address ▲	Device Type	Capabilities	Status
1.3.2.1	1.3.2.1	Workstation	Unknown;	
10.76.91.101	10.76.91.101	Router	Host;	
blrccc2.cisco.com	10.76.91.105	Contact Center Express	Contact Center Express;Media ...	
10.76.91.106	10.76.91.106	Communications Mana...	Communications Manager Expr...	Link Down(F
blrsd1.cisco.com	10.76.91.115	Communications Mana...	Communications Manager;Medi...	Insufficient Fr
blrsd2.cisco.com	10.76.91.116	Communications Mana...	Communications Manager;Medi...	Power Supply
blrcuc1.cisco.com	10.76.91.117	Unity Connection	Unity Connection;Media Server;	Link Down(B
blrmpx.cisco.com	10.76.91.118	Meeting Place Express	Meeting Place Express;	Unresponsive
10.76.91.123	10.76.91.123	Workstation	Unknown;	
blrsd4.cisco.com	10.76.91.124	Workstation	Host;	
10.76.91.125	10.76.91.125	Workstation	Unknown;	
10.76.91.130	10.76.91.130	Switch	Switch;	Link Down(F
msc-bo1-2851.cisco.com	10.76.91.131	Workstation	Host;	
10.76.91.137	10.76.91.137	Voice Gateway	Voice Gateway;Router;H323;M...	Link Down(S

With a look and feel similar to Windows Explorer, the My Network tree helps you keep your complex network organized and performing properly. Devices are automatically organized by device group, and appear in the list in alphabetical order based on the name of the folder or the display name of the device. For more information on the type of information displayed, see Device List, page 2-2.

During discovery, device groups are also created for each subnetwork that is found on the network that was scanned. At the top level of the My Network tree, all devices of the entire scan are contained in the All devices folder. The second folder is the All routers folder and contains all devices that can function as a router. The folders below All devices and All routers are specific device groups that are categorized by associated device rules. You can also define and create your own device groups. For more information on these groups, see Understanding Device Groups, page 2-15.

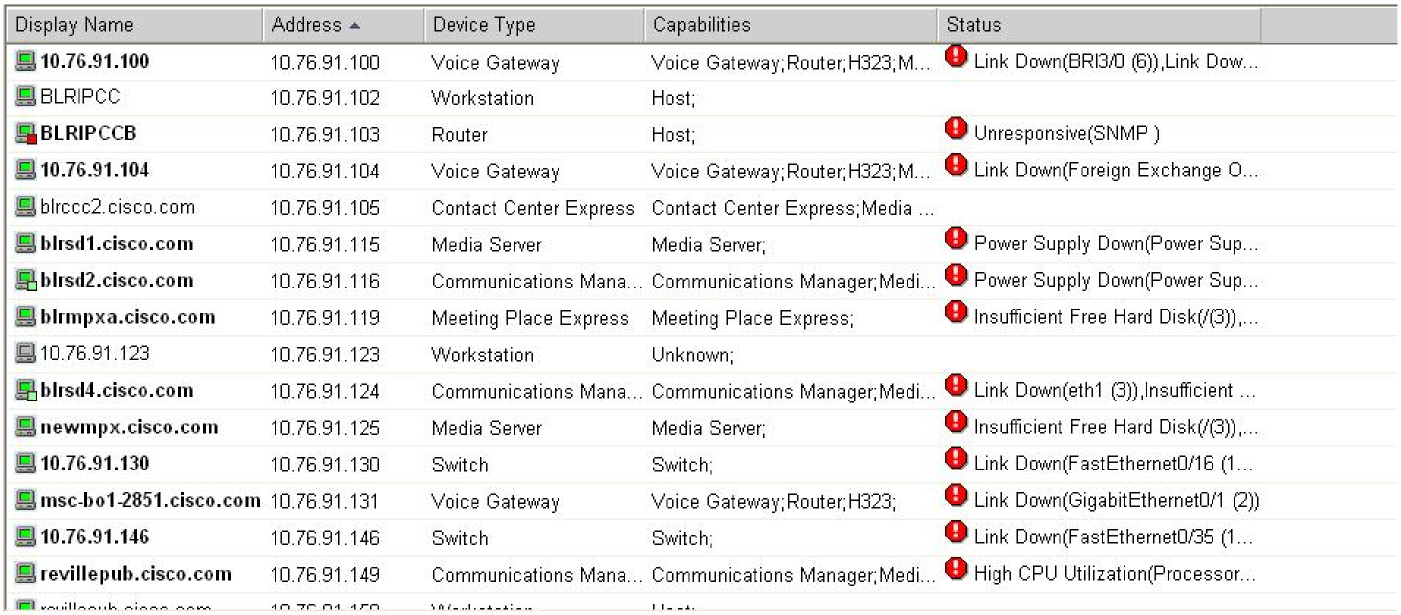
Device List

Each device on the list provides information about its device type, capabilities, and status. The Capabilities column indicates the different roles that the device is capable of. For example, if a device has the capability of being a router and an H323 gateway, the column would list both router and H323 gateway. The Status column describes any faults or events on the device. For a description of each event listed in the Status column, see Appendix A, "Events Processed.".

Note If you right-click a device in the device list to acknowledges its events, all the events for that device are marked as acknowledged. For more information, see Using Acknowledgements, page 2-33.

Figure 2-1 shows an example of a device list.

Figure 2-1 Device List



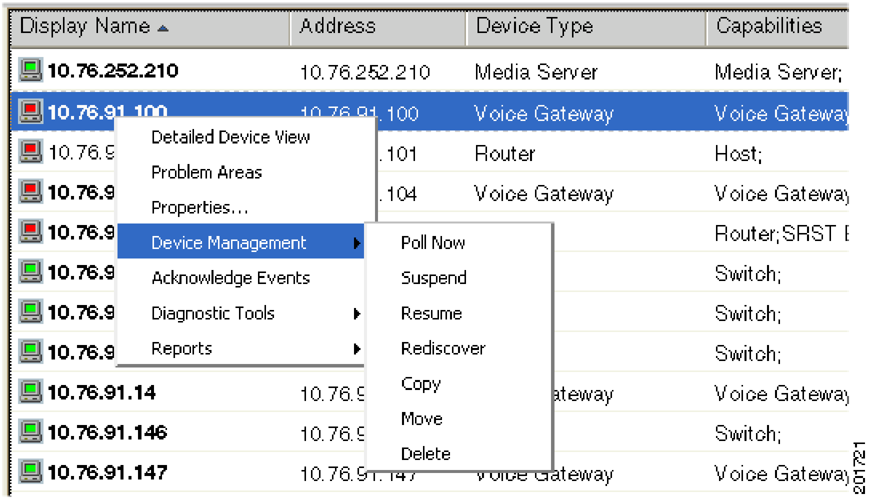
Display Name	Address ▲	Device Type	Capabilities	Status
10.76.91.100	10.76.91.100	Voice Gateway	Voice Gateway;Router;H323;M...	Link Down(BRI3/0 (6)),Link Dow...
BLRIPCC	10.76.91.102	Workstation	Host;	
BLRIPCCB	10.76.91.103	Router	Host;	Unresponsive(SNMP)
10.76.91.104	10.76.91.104	Voice Gateway	Voice Gateway;Router;H323;M...	Link Down(Foreign Exchange O...
blrccc2.cisco.com	10.76.91.105	Contact Center Express	Contact Center Express;Media ...	
blrsd1.cisco.com	10.76.91.115	Media Server	Media Server;	Power Supply Down(Power Sup...
blrsd2.cisco.com	10.76.91.116	Communications Mana...	Communications Manager;Medi...	Power Supply Down(Power Sup...
blrmpxa.cisco.com	10.76.91.119	Meeting Place Express	Meeting Place Express;	Insufficient Free Hard Disk(/(3)),...
10.76.91.123	10.76.91.123	Workstation	Unknown;	
blrsd4.cisco.com	10.76.91.124	Communications Mana...	Communications Manager;Medi...	Link Down(eth1 (3)),Insufficient ...
newmpx.cisco.com	10.76.91.125	Media Server	Media Server;	Insufficient Free Hard Disk(/(3)),...
10.76.91.130	10.76.91.130	Switch	Switch;	Link Down(FastEthernet0/16 (1...
msc-bo1-2851.cisco.com	10.76.91.131	Voice Gateway	Voice Gateway;Router;H323;	Link Down(GigabitEthernet0/1 (2))
10.76.91.146	10.76.91.146	Switch	Switch;	Link Down(FastEthernet0/35 (1...
revillepub.cisco.com	10.76.91.149	Communications Mana...	Communications Manager;Medi...	High CPU Utilization(Processor...
revillepub.cisco.com	10.76.91.150	Workstation	Host;	

Context-Sensitive Menu

A context-sensitive menu is available on the web interface of the Devices tab. The context-sensitive menu comes up when you right-click a device or device group. This menu contains a list of tools that can be used on the device or device group. The type of tools that are available depends on the type of device you have selected. For more information on the standard network tools available, see Launching Network Tools, page 4-13.

Figure 2-2 shows an example of the context-sensitive Menu.

Figure 2-2 Context-Sensitive Menu



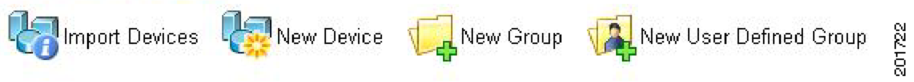
Display Name ▲	Address	Device Type	Capabilities
10.76.252.210	10.76.252.210	Media Server	Media Server;
10.76.91.100	10.76.91.100	Voice Gateway	Voice Gateway
10.76.9	.101	Router	Host;
10.76.9	.104	Voice Gateway	Voice Gateway
10.76.9			Router;SRST I
10.76.9			Switch;
10.76.9			Switch;
10.76.9			Switch;
10.76.91.14	10.76.9	ateway	Voice Gateway
10.76.91.146	10.76.9		Switch;
10.76.91.147	10.76.91.147	Voice Gateway	Voice Gateway

Device Toolbar

The Device Toolbar provides ways for you to add devices and groups.

Figure 2-2 shows an example of the Device Toolbar.

Figure 2-3 Device Toolbar



The Devic Toolbar contains the follwoing:

- **Import Devices.** Imports devices from a file.
- **New Device.** Adds a new device to your list of monitored devices.
- **New Group.** Adds a new device group to your list of monitored devices.
- **New User Defined Group.** Adds a new user-defined group to your list of monitored devices.

Device States and Icons

Each folder in the My Network tree has a device state indicator on the folder icon. This indicator shows the worst state across all of the devices contained in that folder.

The following icons appear in the device list when viewing the contents of a device group.

Icon	Description
🟩	(Green) All monitors on the device are considered up.
🟥	(Red) Device is considered down, because one or more monitors are down. The green square shows that at least one monitor is responding.
🟥	Device entry appears in another device group. At least one monitor on the device is unresponsive, but at least one is considered up.
🟧	(Orange) Device is currently in maintenance mode.
🟥	Device group contains at least one device that is considered down.
▨	Device group is empty, or devices have not been polled due to a dependency on another device.
🟥 **wks**	A bold device name shows that the device has undergone a state change, and that state change has not been acknowledged.

Adding a New Device

Note

- You cannot add new devices to dynamic groups. A device is automatically categorized in Cisco netManager.
- The device will not be added if you have reached the device count limit of your license. If this happens, an appropriate error message will appear when you try to add the device.

- Cisco Discovery Protocol (CDP) must be enabled on a device in order for its network connections to display in the Physical Connectivity View. CDP is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. CDP is enabled by default on Cisco routers. For more information, see http://www.cisco.com/en/US/tech/tk962/technologies_tech_note09186a00801aa000.shtml.
- When a wireless LAN controller is added, not all the lightweight access points registered to it will be shown if you have reached the device count limit of your license. In this situation, an error message will not appear. The log file will indicate this if the trace was enabled.
- Do not cancel while a device scan is in progress. This may add duplicate devices to the system. If duplicate devices are added, manually delete the duplicate device from the Device tab (right-click device and select **Device Management** > **Delete**).

To manually add a new device, use the following procedure. To add multiple devices using a file, see Importing Devices from a File, page 2-9. To use auto discovery, see Using the Device Discovery Wizard, page 2-6.

Step 1 Do one of the following:

- From the Devices tab, right-click the **My Network** folder, and select **New Device**. The Add New Device dialog box opens.
- From the GO menu, select **Device** > **New Device...**.

Step 2 Enter the IP address or hostname for the device you want to add.

Step 3 Click **Advanced** to select a number of additional options for which to scan the device. For more information on the options available from this dialog box, see Active/Performance Monitors Scan Properties.

Step 4 To add a device without scanning, select **Add device immediately without scanning**. This immediately adds a *bare-bones* device, generically categorized as a workstation.

Step 5 Click **OK** to save changes. Cisco netManager attempts to resolve the IP address or hostname, then scans that device for active monitors. When the scan is complete, the Device Properties dialog box opens, allowing you to further configure the device as needed.

Note If you have entered SNMP credentials and the device does not respond to SNMP within the number of retries and timeout as configured globally in GO > Configure > Default SNMP Timeout settings, then the credentials have not been associated with the device. To correct this, right-click the device from the Device List and select **Properties**. Select Credentials and enter the correct credentials in the fields provided. Then try to rediscover the device; see Rediscovering Devices, page 2-14.

Active/Performance Monitors Scan Properties

This dialog box appears when you add devices.

Select the active and performance monitors that you want Cisco netManager to scan for during discovery. After they are discovered, Cisco netManager will configure the new devices with the monitors found.

The top list displays active monitors that have been defined in the Active Monitor Library with the Use in Discovery option selected. The bottom list displays all performance monitors defined in the Performance Monitor Library. For more information about performance monitors, see Chapter 9, “Using Passive Monitors.” The following options are displayed:

- **Use comprehensive discovery**—By default, Cisco netManager sends a ping command to each viable IP address in the range configured in the first section of this wizard. If the device responds, Cisco netManager then scans for the monitors listed on this dialog box. If no device responds, discovery moves on to the next IP address. Select this option to have device discovery scan each IP address for all of the selected monitors without first sending the ping command to the device. Discovery will take longer if this option is selected.

Note If you want a ping monitor created for the devices found in discovery, you must select Ping as an 'active monitor to scan' even if you have cleared the Use comprehensive discovery option.

During discovery, interface monitors are added after the scan, only if a device has multiple physical interfaces. If a device has only one interface, then no interface monitors are added, even if the interface monitor is selected to be scanned. Loopback interface does not count.

- **Resolve host names**. Select this option to have Cisco netManager attempt to populate the list of discovered devices with hostnames, instead of IP addresses. Clear this option to have the list show only IP addresses of discovered devices.
- **Identify device via SNMP**. Select this option to have Cisco netManager read the SNMP information on the device.
- **SNMP read communities**. Enter one or more community strings, separated by commas, that the device will respond to. If the read community string is incorrect, or none is provided, Cisco netManager determines device type based on the monitors discovered during the scan.

Note This option is only available when adding a single device.

- **Windows credentials**. Select a Windows credential to use when attempting to discover devices where you have to provide a Windows username or password when connecting. Credentials are configured in the Credentials Library. When a device is discovered using a credential, that credential is then associated to that device. You can change this on **Device Properties** > **Credentials**. If you select All, discovery uses all configured credentials in the Credentials Library. The credential that is successful is then associated with the device.

Using the Device Discovery Wizard

The Device Discovery wizard scans your network for devices, using the protocols and settings you choose. After devices and monitors are discovered, you select the ones you want to monitor and Cisco netManager creates devices in the database for each item you choose.

The wizard begins when the console is launched and there are no devices on the system.

Note The console is only available from the server where Cisco netManager is installed (**Start > All Programs > Cisco netManager 1.1 > Cisco netManager 1.1 Discovery**).

Device groups are created based on subnetworks discovered during the scan. You may notice that some group folders may be empty. This is because a subnet was discovered, but the devices in that subnet were not scannable or you chose not to monitor them.

Device Discovery Scan Types

There are four options for device discovery. They are:

- **SNMP SmartScan**: SmartScan discovers devices by reading SNMP information on your network. This scan type uses an SNMP-enabled router to identify both network devices and subnetworks. We recommend using SmartScan as your primary Discovery method.
- **IP Range Scan**: Cisco netManager scans a range of IP addresses and finds the devices that respond to one or more of the chosen services. The Discover Devices wizard prompts you to enter a range of the IP addresses in your network. You should use IP Range Scan if SNMP is either unavailable or does not meet your needs.
- **Network Neighborhood**: Scanning a Network Neighborhood creates a list of devices by scanning the Windows network to which your computer is connected, and finding the other systems on the network. Use this type of scan if you only want to discover Windows devices.
- **Hosts File Import**: Cisco netManager imports devices from the system's Hosts file, which is a text file that lists hostnamess and their IP addresses on a network. For small networks, the Hosts file is an alternative to DNS. The Hosts file may also be called a host table by some TCP/IP vendors.

Device Discovery Example

This example describes how to use the Device Discovery wizard with the SNMP SmartScan option to discover devices.

In this example, you want to discover all of the devices attached to a specific SNMP-enabled router on your network. To accomplish this, you need to:

- Know the IP address of the SNMP-enabled router whose network you want to discover.
- Know the Read Community name assigned to the devices on the network.

To discover devices:

Step 1 The Device Discovery Wizard is only available from the Cisco netManager console. The console is only available from the server where Cisco netManager is installed (**Start > All Programs > Cisco netManager 1.1 > Cisco netManager 1.1 Discovery**).

Step 2 From the console, select **File > Discover Devices**. The New Device Discovery Wizard appears.

Step 3 Select SNMP SmartScan as the method for scanning your network, then click **Next**. The SNMP SmartScan settings dialog boxopens.

Step 4 In the SNMP enabled router box, enter the IP address of the SNMP-enabled router you want to use for this scan.

Step 5 In the SNMP read communities box, enter the proper read community string for that router. If an incorrect string is entered, Cisco netManager will be unable to scan the network. Additional community strings may be entered, separated by commas, if there are multiple SNMP-enabled devices on your network that use different strings.

Optionally, select the Windows credentials that you want to use during discovery. These credentials are configured in the Credentials Library, and store Windows authentication information (username and password) for those devices that require a login for discovery or monitoring. Click the Browse (**...**) button next to this box to access the Credentials Library. You can select a specific credential, select **All** to try all credentials that are configured or select **None** to ignore those devices that require you to log on. The credential that is successful is associated with each device.

Step 6 Click the **Advanced** button if you want to change the scan's default timeouts in milliseconds, retry counts, and scan depth.

- Click the **Limit scan to IP class of root device** option if you want to limit the scan to the network class (A, B, or C) defined by the IP address of the root device. If the IP address is within the network class of the root device, the scan proceeds. Otherwise, the scan skips to the next IP address.
- Click the **Resolve host names** option if you want to populate the list of discovered devices with hostnames in addition to IP addresses.
- Click **OK** to save changes and return to the SNMP SmartScan settings dialog box.

Step 7 Click **Next**. The Active/Performance Monitors to Scan dialog box opens. Select the type of active and performance monitors you want to use in this scan process. For this example, let's select Ping and HTTP as the active monitors and Disk Utilization as the performance monitor to be used in the scan process.

- The *Ping monitor* polls the device on a regular basis to establish whether it is up or down. By default, Cisco netManager sends a ping command to each viable IP address in the range configured during the first section of this wizard. If the device responds, Cisco netManager scans for the monitors listed on this dialog box. If the device does not respond, discovery moves on to the next IP address. You can select **Use comprehensive discovery** to have device discovery scan each IP address for all of the selected monitors without first sending the ping command to the device. Discovery takes longer if this option is selected.

Note If you want a Ping monitor created for the devices found in discovery, you must select **Ping** as an active monitor to scan even if you have cleared the Use comprehensive discovery option.

Note If a device only has one interface, Cisco netManager intentionally does not add the Interface Active Monitor during discovery. Doing so with the Ping Active monitor would be redundant.

- The *HTTP monitor* polls a web server (if one is discovered) on the device on a regular basis to establish if it is up or down.

Tip To see how a monitor is configured, you can go to the Active Monitor Library (**Configure > Active Monitors**), select a monitor, and click **Edit**.

- The *Disk Utilization monitor* monitors and reports on the available disk space for the selected device. Data collected is displayed in the Disk Utilization Report.

Step 8 Click **Next**. The Device Discovery window displays the estimated remaining scan time and the scan's progress. To cancel device discovery, click **Stop**.

Step 9 When the discovery is complete, the Devices to Monitor window opens, listing all of the devices just discovered. Note that if any of the devices have already been entered into the database, a shortcut to the device will be created in the device list. To add all of the devices to the database, click **Next**. To remove specific devices to be monitored from this list, clear the check box next to the device you want to remove.

Note Not all discovered devices that appear in the list will be added to the database if you have reached the device count limit of your license. To verify which devices have been added, go to the device list.

Note Additional active monitors and performance monitors that are already in the database will not be added to devices.

Step 10 Click **Next**. The Action Policy Selection dialog box opens. For more information about action policies, see the About Action Policies, page 6-21.

Step 11 Complete the remaining screens in the wizard.

The Results summary shows the number of selected new devices, number of active and performance monitors, whether or not an Action Policy is applied, and the number of selected device shortcuts.

Step 12 Click **Finish** to begin monitoring the devices. A progress bar appears while devices are being added to the database, then the Device View opens.

Note If some device group folders are empty, it is because although a subnet was found, either the devices in the subnet were either not scannable, or you chose not to monitor them.

About IP Phone Discovery

Cisco netManager performs an auto-discovery on all IP phones every four hours to detect if SIP and SCCP IP Phone are associated with a managed Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. Cisco netManager also verifies registration status of all detected IP phones with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

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

Importing Devices from a File

Step 1 Do one of the following:

- From the Device tab, click the **Import Device** icon located in the Device Toolbar.

- From the GO menu, select **Device > Import Devices...**.

Step 2 Select either Server or Local.

If you select Server, you only need to enter the filename; for example, seed.csv. The file is assumed to be present in the <CNM_Install_Dir>\importFiles directory.

If you select Local, enter the full path of where the file can be found, or browse the file system and select the file using the Browse button.

Step 3 Enter the filename or browse the file system and select the file using the Browse button.

Note Only CSV2.0 and CSV3.0 file formats are supported. XML files are not supported. For more information on file format, see Sample CSV Files, page 2-10.

Step 4 Click **Advanced** to select a number of additional options for which to scan the device. For more information on the options available from this dialog box, see Active/Performance Monitors Scan Properties, page 2-5.

Step 5 Click **OK** to save changes. Cisco netManager attempts to resolve the IP address or hostname, then scans that device for active monitors. When the scan is complete, the Device Properties dialog box opens, allowing you to further configure the device as needed.

Note When a device cannot be added because the device count limit has been reached (due to the type of license purchased), the progress bar will indicate the number of devices not added. The Import Status window will also have this information.

Sample CSV Files

Sample CSV 2.0 File

```
;
; This file is generated by the export utility
; If you edit this file, be sure you know what you are doing
;
Cisco Systems NM data import, source = export utility; Version = 2.0;
Type = Csv
;
; Here are the columns of the table.
;   Columns 1 and 2 are required.
;   Columns 3 through 19 are optional.
; Col# = 1: Name (including domain or simply an IP)
; Col# = 2: RO community string
; Col# = 3: RW community string
; Col# = 4: Serial Number
; Col# = 5: User Field 1
; Col# = 6: User Field 2
; Col# = 7: User Field 3
; Col# = 8: User Field 4
; Col# = 9; Name = Telnet password
; Col# = 10; Name = Enable password
; Col# = 11; Name = Enable secret
; Col# = 12; Name = Tacacs user
; Col# = 13; Name = Tacacs password
; Col# = 14; Name = Tacacs enable user
; Col# = 15; Name = Tacacs enable password
; Col# = 16; Name = Local user
; Col# = 17; Name = Local password
; Col# = 18; Name = Rcp user
; Col# = 19; Name = Rcp password
;
; Here are the rows of data.
;
123.45.118.156,public,,FHH080600dg,,,,,,,,,,,,,,,
123.45.118.150,public,,FHH0743W022,,,,,,,,,,,,,,,
10.88.13.18,public,,,,,,,,
10.88.13.65,public,,,,,,,,
10.88.11.175,public,,,,,,
10.88.11.124,public,,,,,,
10.88.11.153,public
```

Sample CSV 3.0 File

```
; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV; Version=3.0

;
;Start of section 0 - Basic Credentials
;
;HEADER:
management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_d
evice_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,rxboot_mode_username,rxb
oot_mode_password,primary_username,primary_password,primary_enable_password,http_username,
http_password,http_mode,http_port,https_port,cert_common_name
;
123.10.118.84,,,,123.10.118.84,unknown,0,999980341,public,,,,,,,,,,,administrator,cisco,ht
tp,80,,
10.16.83.82,10.76.93.82,,,srst-sw,unknown,0,279568149,public,private,,,,,,,,,,,,,,,
10.16.81.71,10.76.91.71,,,10.16.91.71,unknown,0,268437969,public,,,,,,,,,,,,,,,,
10.16.81.183,10.76.91.183,,,10.76.81.183,1.3.6.1.4.1.9.1.26,0,268437597,public,,,,,,,,,,,,
,,,,
10.16.83.75,,,,ipif-skate.cisco.com,unknown,,999990341,public,,,,,none,,,Administrator,voi
ce,,Administrator,voice,,,,
10.16.81.30,10.76.91.30,,,10.16.81.30,unknown,0,268437960,public,,,,,,,,,,,,,,,,
10.16.81.146,10.76.91.146,,,10.16.81.146,unknown,0,278546113,,,ipcom,ipcom,,MD5,,,,,,,,,,,
10.16.81.72,10.76.91.72,,,10.16.81.72,unknown,0,268437990,public,,,,,,,,,,,,,,,,
123.20.118.3,,,,172.20.118.3,unknown,0,268437990,public,,,,,,,,,,,,,,,,
10.16.81.149,10.16.81.149,,,10.16.81.149,unknown,0,999990341,public,private,,,,none,,
Administrator,cisco,,Administrator,cisco,,,,
```

Sample of a List of IP Addresses

```
10.16.83.18,
10.16.83.65,
10.16.81.175,
10.16.81.124,
10.16.81.153,
10.16.81.130,
10.16.81.151,
10.16.81.67,
10.16.81.83
```

Configuring Network Interfaces on a Device

The Network Interface dialog box displays all network interfaces currently configured for the device. Cisco netManager monitors all interfaces listed here, displaying the worst state of the interfaces as the device status.

Step 1 From the device list, right-click a device, then click **Properties**. The Device Properties dialog box opens.

Step 2 Click **General**. The General dialog box opens.

Step 3 Click **Additional Network Interfaces**. The Add Network Interfaces dialog box opens.

Step 4 Do one of the following:

- Click **Add** to add a network interface. Enter the network information for the new interface.
- Click **Set Default** to change the default network interface on a device. Select the interface you want to make the default.
- Click **Edit** to modify the interface details.
- Click **Remove** to remove the interface.

Step 5 Click **OK** to return to the General section.

Configuring Credentials

The Credentials system stores login or community string information for Windows (WMI active monitors and WMI performance monitors) and SNMP devices in the Cisco netManager database. The system supports SNMPv1 and SNMPv2.

Credentials are configured in the Credentials Library (found on the web interface menu at **GO > Configure > Credentials Library**) and used in several places throughout the application. They can be associated to devices from **Device Properties > Credentials** or through the **Credentials Bulk Field Change** option.

A device needs SNMP credentials applied to it before SNMP-based active monitors will work. Similarly, NT Service Checks must have Windows credentials applied.

Editing SNMP Timeout and Retries

If an SNMP query does not respond in time, Cisco netManager will time out. It will then retry contacting the device for as many times as listed under the snmpretries attribute in the configuration file. The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, Cisco netManager waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry. The SNMP timeout and retries are global settings.

Step 1 Select **GO** > **Configure** > **Default SNMP Timeout**.

Step 2 Enter the following:

- **Timeout** (milliseconds)—Enter the timeout in milliseconds (ms). If a device does not respond to the scan within this time, the scan continues to the next IP address. The timeout should be set to 300 ms or greater.
- **Retry count**—This is the number of times to try to discover a device at a given IP address, before continuing to the next device.

Adding Attributes to a Device

Step 1 From the device list, right-click a device, then click **Properties**. The Device Properties dialog box opens.

Step 2 Click **Attributes**. The Attributes dialog box opens.

Step 3 Do one of the following:

- Click **Add** to add a new device attribute. The Add Attribute dialog box opens.
- Select a device attribute in the list, then click **Edit** to change the settings.
- Select a device attribute in the list, then click **Remove** to remove it from the list.

Step 4 Enter information in the Attribute name and Attribute value boxes.

Step 5 Click **OK** to save changes.

Adding Notes to a Device

Step 1 From the device list, right-click a device, then click **Properties**. The Device Properties dialog box opens.

Step 2 Click **Notes.** The Notes dialog box opens.

Step 3 Enter the note in the **Notes** dialog box.

The first line of the Notes box displays information about when the device was added to the database. If viewing the notes on a shortcut, the date and time the device was added to the database are displayed.

You can customize the notes with any information you want to include about the device. For example, you may want to record historical information about a device, physical location information, or notes relating to the actions configured for the device.

Note There is no automatic word wrap. Add a return to display information in the dialog box without requiring scrolling to view it.

Step 4 Click **OK** to save changes.

Changing a Device IP Address

Step 1 From the device list, right-click a device, then select **Properties** > **General**.

Step 2 Enter the new IP address in the Address box.

Step 3 Click **OK** to save changes.

Changing a Device Name

Changing the name of a device changes how it appears in the list views.

Step 1 From the device list, right-click a device. From the context menu, click **Properties > General**.

Step 2 In the General section of Device Properties, enter the new name in the Display Name box.

Step 3 Click **OK** to save changes.

Rediscovering Devices

This task rediscovers all the devices in the network. You would want to perform this task if device credentials, capabilities, etc., are changed. During rediscovery, if device capabilities have changed, associated monitors and data inventory are updated. If a device is unreachable, the device status will be updated accordingly. This can be a time-consuming task that will allow you navigate the web interface, but not perform any operations.

To rediscover devices:

Step 1 From the GO menu, select **Device > Rediscover Devices...**

Step 2 Click **OK**.

Note If you cannot rediscover a device’s new capabilities because you have reached the device count limit of your license, an appropriate error message will appear.

Suspending and Resuming Single Device Polling

This task permanently suspends or resumes polling on a specific device.

Step 1 From the device list, right-click a device. From the context menu, click **Device Management > Suspend** or **Device Management > Resume**.

Step 2 Click **OK**.

Understanding Device Groups

A group consists of objects, where objects refer to devices. Each group has a set of properties (such as a name, description, permission, and so on), but what define a group are its associated rules. Rules determine the membership of a group, which may change whenever the rule is evaluated.

The following types of groups are supported:

- **System-Defined groups**—The default grouping of devices that cannot be deleted or edited. For a description of each system-defined group, see the Working with System-Defined Groups, page 2-15.
- **Dynamic groups**—A dynamic group that you can create by defining an SQL query. Dynamic groups act as SQL queries that run on the Cisco netManager database, and can display real-time data if viewed through a report that is set to automatically refresh. For more information on dynamic groups, see the Using Dynamic Groups, page 2-17.
- **User-Defined groups**—A dynamic group where the user can group devices using one of the following criteria: location, description, contact or IP address. To create a user-defined group, see Creating a User-Defined Group, page 2-17.

Note The supported format for an IP address is a set of four octets (*.*.*.*). An asterisk (*) denotes the octet range of 1-255. You can filter IP addresses using the octets in a sequential order. For example, if you filter devices with IP addresses containing 10.76.91, your results may include 10.76.91.151 or 172.10.76.91. You cannot use an IP range or wildcards, for example 10.*.91.

- **Static groups**—Groups that you edit or create to reflect the way you manage the network. You can edit or create device groups and determine whether they can be viewed by other users. To create a static group, see Creating a Device Group, page 2-16.

Working with System-Defined Groups

The system-defined groups are visible to all users, and are the default groups that are administered by Cisco netManager. If a device has multiple capabilities, the device will be listed under all appropriate groups. For example, if a device can function as a router, H323 gateway and a MGCP gateway, it will be listed in all those groups.

Note System-defined groups cannot be modified or deleted.

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

The following system-defined groups come preconfigured:

- Routers
- Switches

- Hosts
- Servers
- Cisco Media Server
- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Cluster. Lists subgroups of the Cisco Unified Communications Manager cluster group and contains all of the devices associated with the corresponding instance of the Cisco Unified Communications Manager cluster.
- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- Cisco Unified Communications Manager Express
- Cisco Unified Conferencing for TelePresence
- Cisco Unified Contact Center Express
- Cisco Unified Communications Manager Business Edition
- H323 Gateways
- MGCP Gateways
- SRST Devices
- Wireless LAN Controllers
- Autonomous Access Points
- Security Devices

Creating a Device Group

To create a static device group:

Step 1 Do one of the following:

- From the My Network tree in the Device tab, right-click a folder, and select **New Group...**.
- Click the **New Group** icon located on the top right of the Device tab.

Step 2 Enter the name of the new group you are creating.

Step 3 Enter the description for the new group.

Step 4 Click **OK**.

Modifying Group Properties

Step 1 Do one of the following:

- From the My Network tree in the Device tab, right-click a folder, and select **New Group...**.
- Click the **New Group** icon located on the top right of the Device tab.

Step 2 Modify the name of the group.

Step 3 Modify the description of the group.

Step 4 If you are modifying a dynamic group, select appropriate user access privileges for that group.

Step 5 Click **OK**.

Creating a User-Defined Group

Step 1 From the My Network tree in the Device tab, right-click **User Defined Group** folder, and select **New User Defined Group...**.

Step 2 Enter the name of the new group you are creating.

Step 3 Enter a description for the new group.

Step 4 Select the attribute that will be used to filter devices for the group; for example, location.

Step 5 Enter the attribute value; for example, California.

Step 6 Click **OK.**

Modifying Group Access Rights for a User

Step 1 From the My Network tree in the Device tab, right-click **User Defined Group** folder, and select **Properties**.

Step 2 Check the appropriate Read/Write access rights.

Step 3 Click **OK**.

Renaming a Device Group

To rename a device group, right-click the group in the My Network tree, click **Properties**, then change the name in the Group Name box.

Using Dynamic Groups

This feature provides the ability to create device groups based on whatever criteria users choose, without having to create device shortcuts. Dynamic groups can be created for specific device types, device attributes, active monitors, or anything else that is stored for individual devices in the database. Dynamic groups act as SQL queries that run on the Cisco netManager database, and can display real-time data if viewed through a report that is set to automatically refresh.

Cisco netManager is preconfigured with dynamic group examples. You can view these examples from the Dynamic Group Examples folder, under the My Network tree in the Devices tab.

All of the Dynamic Group Examples are active, so if you have devices that meet the criteria, you will see the device displayed within the group. In the web interface, the dynamic group display is refreshed every 2 minutes. A group is also refreshed when you select it.

To view or edit the criteria for a dynamic group, right-click the group name, then select **Properties**.

Note Dynamic groups on the web interface do not follow group access rights. Anyone with the ability to view the device group that a dynamic group is in can access that dynamic group. However, only devices that the user has the permission to view appear in the group.

Creating Dynamic Groups

To configure dynamic groups:

Step 1 From the My Network tree in the Device tab, right-click a folder, then select **New Dynamic Group**. The Dynamic Group dialog box opens.

Step 2 Select a method for configuring the new Dynamic Group. You can use either the Dynamic Group Builder, or the SQL dialog. If you are an advanced SQL user, you should choose the second option. Otherwise, we recommend selecting the Dynamic Group Builder.

Step 3 Enter the appropriate information into the following fields:

- **Group Name**—Enter a name for the dynamic group as it will appear in the Device List.
- **(Optional) Description**—Enter a short description for the new dynamic group.

In the second part of the dialog box, you will create and edit rules to form an SQL filter for the dynamic group.

Step 4 Click **Add**. The Dynamic Group Rule Editor appears.

In the Dynamic Group Rule Editor, enter the appropriate information. As you create rules, they are added to the Dynamic Group Builder dialog box where you can add more rules, or edit or delete existing rules by clicking the Add, Edit, or Delete buttons.

Parentheses (single, double, triple, and quadruple) are available for use in your filter code. Add them by selecting them from the lists before and after your rules.

You can move existing rules up or down within your filter code by selecting a rule and then clicking on the Up and Down buttons.

Step 5 Click **OK** to add the group to the device list. SQL validation occurs as soon as you click OK. If the filter fails, an error message appears.

In addition to the preconfigured dynamic groups, there are several sample filters available to you to create some dynamic groups.

Tip If you do not know how to formulate SQL queries, you can cut and paste filter entries from existing dynamic groups, then edit them to read data from other tables.

Validating Your Filter Code

Keep in mind that as you configure your rules, the SQL filter is displayed at the bottom of the Dynamic Group Builder dialog box. When you are satisfied with the filter code that is displayed, click the **Validate** button to test the filter. If it runs as you expect, click **OK** to save the configured SQL filter and to add the new dynamic group to your device list. If the code does not run as you expect, but you would still like to save the filter code so that you may edit it at a later time, click **OK**. You can then select the Dynamic Group from the device list and right-click, then select **Properties** to edit the group filter code.

Converting Your Filter Code

You can convert a dynamic group created with the Dynamic Group Builder to the SQL dialog box by clicking the **Convert** button. It is important to note that once you convert the dynamic group to the SQL dialog box, you will not be able to edit the group in the Dynamic Group Builder again - you will only be able to make changes to the group from the SQL dialog box. If you aren't an advanced SQL user, we recommend that you make a copy of thedynamic group so that you can keep a copy available for editing in the Dynamic Group Builder.

To use the SQL Dynamic Group dialog box:

Step 1 Enter a Display name for the group, enter the group Description, and enter an SQL query in the Filter box that identifies the devices you want to appear in that group.

Step 2 Click **OK** to add the group to the device list. SQL validation occurs as soon as you click OK. If the filter fails, an error message appears.

Dynamic Group Rule Editor

This is the second dialog box of the Dynamic Group Builder. Use this dialog box to create or edit rules for use in the new group's SQL filter.

Step 1 Select the desired rule components from the list and enter a variable in the empty field.

Step 2 Click **OK** to add the rule to the Dynamic Group Builder dialog box.

Dynamic Group Examples

The following table lists several dynamic group filters that you can use to create dynamic groups for your devices. To use these examples, select the text of the filter, and then copy and paste the text into the Filter box of the Dynamic Group dialog box.

Note If the copyright information appears in the text that you copied and pasted from the filter, you should delete it.

Description	Filter
Shows all devices that have had a state change in the last three hours.	SELECT DISTINCT Device.nDeviceID FROM Device JOIN PivotActiveMonitorTypeToDevice ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID JOIN ActiveMonitorStateChangeLog ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID = ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID WHERE ISNULL(Device.bRemoved, 0) = 0 AND DATEDIFF(hh, ActiveMonitorStateChangeLog.dStartTime, GETDATE()) <= 3
Shows all devices with multiple interfaces.	SELECT DISTINCT NetworkInterface.nDeviceId FROM Device JOIN NetworkInterface ON Device.nDeviceId = NetworkInterface.nDeviceId WHERE ISNULL(Device.bRemoved,0) = 0 GROUP BY NetworkInterface.nDeviceId HAVING COUNT(NetworkInterface.nDeviceId) > 1
Shows all devices that have gone down in the last few hours.	SELECT DISTINCT Device.nDeviceID FROM Device JOIN PivotActiveMonitorTypeToDevice ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID JOIN ActiveMonitorStateChangeLog ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID = ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID JOIN MonitorState ON Device.nWorstStateID = MonitorState.nMonitorStateID WHERE ISNULL(Device.bRemoved, 0) = 0 AND DATEDIFF(hh, ActiveMonitorStateChangeLog.dStartTime, GETDATE()) < = 2 AND MonitorState.nInternalMonitorState !=3

Shows all device groups (except itself) in a rotating order. For example, if the State Change Timeline report is using this rotating group, every minute, when the report auto-refreshes (or when the user presses F5), this rotating group looks at a different dynamic group. So, it might look at Dynamic Group A first, then B, then C, etc., and then start back at the beginning. The effect is like a security guard's monitor: The scene changes from the front door, to the back door, to the loading dock, to the hallway, back to the front door, etc.
Note the comments in the code.
	-- The name of *this* dynamic group. This variable *must* be set
	-- the what you name this Group via the console.
	DECLARE @sGroupNameThis NVARCHAR(150)
	SET @sGroupNameThis = 'My Rotating Group'
	-- Figure out which other Dynamic Group to do next. Note that
	-- this section could be modified to use any criteria you want
	-- to select Dynamic Groups to rotate through.
	DECLARE @sGroupNamePrev NVARCHAR(150)
	SELECT @sGroupNamePrev = sNote
	FROM DeviceGroup
	WHERE sGroupName = @sGroupNameThis
	DECLARE @sGroupNameNext NVARCHAR(150)
	SELECT TOP 1 @sGroupNameNext = sGroupName
	FROM DeviceGroup
	WHERE sGroupName > @sGroupNamePrev AND
	ISNULL(bDynamicGroup,0) != 0
	AND sGroupName != @sGroupNameThis
	ORDER BY sGroupName ASC
	-- Reached the end? Start over at beginning.
	IF ISNULL(@sGroupNameNext,'') = ''
	BEGIN
	SELECT TOP 1 @sGroupNameNext = sGroupName FROM DeviceGroup
	WHERE ISNULL(bDynamicGroup,0) != 0
	AND sGroupName != @sGroupNameThis
	ORDER BY sGroupName ASC
	END
	-- Update which Group we just displayed, so that next time
	-- we know which Group to start after. As far as I know, the
	-- 'sNote' column is unused.
	UPDATE DeviceGroup SET sNote = @sGroupNameNext
	WHERE sGroupName = @sGroupNameThis -- Execute the next Group.
	DECLARE @sFilter NVARCHAR(3000) SELECT @sFilter = sFilter
	FROM DeviceGroup
	WHERE sGroupName = @sGroupNameNext
	EXEC (@sFilter)

Description	Filter

If there are any rows in the GeneralErrorLog table in the last 24 hours, then all devices will appear in this Dynamic Group; if there aren't, then no devices appear.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`WHERE ISNULL(Device.bRemoved, 0) = 0`
	`AND EXISTS (SELECT *`
	`FROM GeneralErrorLog`
	`WHERE DATEDIFF(hh, dDateTime, GetDate()) <24)`

Shows all the devices (in one specific group) that had an action fire in the last three hours.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`JOIN ActionActivityLog`
	`ON Device.nDeviceId = ActionActivityLog.nDeviceId`
	`WHERE ISNULL(Device.bRemoved, 0) = 0`
	`AND DATEDIFF(hh, ActionActivityLog.dDateTime, GETDATE()) < = 3`
	`AND Device.nDeviceId IN`
	`(SELECT nDeviceId`
	`FROM PivotDeviceToGroup`
	`WHERE nDeviceGroupId =`
	`(SELECT nDeviceGroupId`
	`FROM DeviceGroup`
	`WHERE sGroupName = 'My Key Resources Group'`

Shows all devices that need acknowledgement.	`SELECT DISTINCT Device.nDeviceID FROM Device JOIN`
	`PivotActiveMonitorTypeToDevice`
	`ON Device.nDeviceID =`
	`PivotActiveMonitorTypeToDevice.nDeviceID JOIN`
	`ActiveMonitorStateChangeLog`
	`ON`
	`PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =`
	`ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID`
	`WHERE ISNULL`
	`(Device.bRemoved,0) = 0 AND ISNULL`
	`(ActiveMonitorStateChangeLog.bAcknowledged, 0) = 0 AND`
	`PivotActiveMonitorTypeToDevice.bRemoved!=1`

Shows all of the Cisco devices.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`WHERE ISNULL(Device.bRemoved,0) = 0`
	`AND sSnmpOID LIKE '1.3.6.1.4.1.9%'`

Shows all devices whose disks are 90 percent full.	`SELECT DISTINCT Device.nDeviceID`
	`--, Device.sDisplayName, nUsed_Avg / NULLIF(nSize, 0) As`
	`nPercentFull`
	`FROM Device`
	`JOIN PivotStatisticalMonitorTypeToDevice`
	`ON Device.nDeviceID =`
	`PivotStatisticalMonitorTypeToDevice.nDeviceID`
	`JOIN StatisticalDiskCache`
	`ON`
	`PivotStatisticalMonitorTypeToDevice.nPivotStatisticalMonitorTypeTo`
	`DeviceID =`
	`StatisticalDiskCache.nPivotStatisticalMonitorTypeToDeviceID`
	`WHERE Device.bRemoved = 0`
	`AND StatisticalDiskCache.nDataType = 1`
	`AND nUsed_Avg / NULLIF (nSize, 0) > 0.90`

Shows all down or maintenance devices (of specified device types) with at least one active monitor down.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`JOIN MonitorState`
	`ON Device.nWorstStateID = MonitorState.nMonitorStateID`
	`WHERE Device.bRemoved = 0`
	`AND MonitorState.nInternalMonitorState IN (1,2)`
	`AND Device.nDeviceTypeID IN (3,4,38,63,64, 65, 66, 67, 68, 71, 72)`

Description	Filter
Shows only devices on which all active monitors are down.	SELECT DISTINCT Device.nDeviceID FROM Device JOIN MonitorState ON Device.nWorstStateID = MonitorState.nMonitorStateID WHERE Device.bRemoved = 0 AND MonitorState.nInternalMonitorState = 1 AND Device.nWorstStateID = Device.nBestStateID
Shows only those devices on which all active monitors have been down for 20 minutes.	SELECT DISTINCT Device.nDeviceID FROM Device JOIN MonitorState ON Device.nWorstStateID = MonitorState.nMonitorStateID WHERE Device.bRemoved = 0 AND MonitorState.nInternalMonitorState = 1 AND Device.nWorstStateID = Device.nBestStateID AND MonitorState.nInternalStateTime = 20
Displays devices whose actions (or whose active monitors' actions) have a specific word in their name.	SELECT DISTINCT Device.nDeviceID FROM Device JOIN ActionPolicy ON Device.nActionPolicyID = ActionPolicy.nActionPolicyID JOIN PivotActionTypeToActionPolicy ON ActionPolicy.nActionPolicyID = PivotActionTypeToActionPolicy.nActionPolicyID JOIN ActionType ON PivotActionTypeToActionPolicy.nActionTypeID = ActionType.nActionTypeID WHERE Device.bRemoved = 0 AND ActionType.sActionTypeName LIKE '%Critical%' UNION SELECT DISTINCT Device.nDeviceID FROM Device JOIN PivotActiveMonitorTypeToDevice ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID JOIN ActionPolicy ON PivotActiveMonitorTypeToDevice.nActionPolicyID = ActionPolicy.nActionPolicyID JOIN PivotActionTypeToActionPolicy ON ActionPolicy.nActionPolicyID = PivotActionTypeToActionPolicy.nActionPolicyID JOIN ActionType ON PivotActionTypeToActionPolicy.nActionTypeID = ActionType.nActionTypeID WHERE Device.bRemoved = 0 AND PivotActiveMonitorTypeToDevice.bRemoved = 0 AND ActionType.sActionTypeName LIKE '%Critical%'
Shows only devices with a particular Performance Monitor.	SELECT DISTINCT Device.nDeviceID FROM Device JOIN PivotStatisticalMonitorTypeToDevice ON Device.nDeviceID = PivotStatisticalMonitorTypeToDevice.nDeviceID JOIN StatisticalMonitorType ON StatisticalMonitorType.nStatisticalMonitorTypeID = PivotStatisticalMonitorTypeToDevice.nStatisticalMonitorTypeID WHERE Device.bRemoved = 0 AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1 AND StatisticalMonitorType.sStatisticalMonitorTypeName LIKE 'X'

Description	Filter

Shows only devices with a particular passive monitor.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`JOIN PivotPassiveMonitorTypeToDevice`
	`ON Device.nDeviceID = PivotPassiveMonitorTypeToDevice.nDeviceID`
	`JOIN PassiveMonitorType`
	`ON PassiveMonitorType.nPassiveMonitorTypeID =`
	`PivotPassiveMonitorTypeToDevice.nPassiveMonitorTypeID`
	`WHERE Device.bRemoved = 0`
	`AND PivotPassiveMonitorTypeToDevice.bRemoved = 0`
	`AND PassiveMonitorType.sMonitorTypeName LIKE 'X'`

Shows only devices with a particular active monitor.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`JOIN PivotActiveMonitorTypeToDevice`
	`ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID`
	`JOIN ActiveMonitorType`
	`ON ActiveMonitorType.nActiveMonitorTypeID =`
	`PivotActiveMonitorTypeToDevice.nActiveMonitorTypeID`
	`WHERE Device.bRemoved = 0`
	`AND PivotActiveMonitorTypeToDevice.bRemoved = 0`
	`AND ActiveMonitorType.sMonitorTypeName LIKE 'X'`

Finds a device by display name, IP address, or hostname.	`SELECT DISTINCT Device.nDeviceID`
	`FROM Device`
	`JOIN NetworkInterface ON Device.nDeviceID =`
	`NetworkInterface.nDeviceID AND Device.nDefaultNetworkInterfaceID =`
	`NetworkInterface.nNetworkInterfaceID`
	`JOIN DeviceType ON Device.nDeviceTypeID = DeviceType.nDeviceTypeID`
	`WHERE (Device.sDisplayname LIKE 'X' OR`
	`NetworkInterface.sNetworkName LIKE 'X' OR`
	`NetworkInterface.sNetworkAddress LIKE 'X')`
	`AND Device.bRemoved = 0`
	`ORDER BY Device.nDeviceID`

Creating Access Rights for a Device Group

An important part of creating a device group is configuring the appropriate access rights for that group. Group access rights ensure that only those users with specific rights are allowed to view and modify a device group.

Step 1 From the My Network tree in the Device tab, right-click a group, and select **Properties**.

Step 2 From the Group Properties dialog box, you can add and edit the access rights for the selected group. For more information on the types of tasks associated with each access right, see User Access Rights for a Device Group, page 2-24.

Note You must enable group access rights for a user account before a user can add or edit access rights for a device group. To do this, the Cisco netManager administrator will have to enable group access rights for a user in the Manage Users dialog box (**Configure** > **Manage Users**).

User Access Rights for a Device Group

Device Group Access Rights lets the administrator determine which device groups certain web users are allowed to view or edit.

The following is a list of operations and the group access rights that must be assigned for the user to perform those operations:

- List, Map, and Group reports in the Group Views menu require Group Read access.
- Create Group and Group Properties in the Group Operations menu require Group Read Write access.
- Copy Group requires Group Read in the source group, and Group Read Write in the destination group. (Permissions to groups and subgroups are copied, not inherited from the new parent).
- Move Group requires Group Read Write in both the source and the destination groups. (Permissions of the group and subgroups remain the same.)
- Delete Group requires Group Read Write, Device Read Write recursively. (Device Read Write may not be required if the group is empty).
- Create Device requires Group Read Write and Device Read Write. If the device already exists in other groups, you must also have Group Read Write and Device Read Write in one or more of those groups.
- Copy Device requires Group Read in the source group and Group Read Write in the destination group. The level of device permissions must be the same in both groups. Downgrade from Device Read Write to Device Read is also permitted.
- Move Device requires Group Read Write in both the source and the destination groups. The level of device permissions must be the same in both groups. Downgrade from Device Read Write to Device Read is also permitted.
- View Device Properties and Device Reports requires Device Read.
- Modify Device Properties, Bulk Field Change, and Acknowledgement require Device Read Write.

Understanding Device Properties

You can modify individual device properties by right-clicking a device in the Device List, then selecting **Properties**.

The Device Summary page displays basic information about a device, including:

- **Display Name**—Displays the identifying name for the current device. This name is populated during discovery, but can be changed by the user at any time in the Device Properties - General page. Changing the name will not change how the device is polled; it affects only how it is displayed in Cisco netManager.
- **Device Type**—Displays the type of device (printer, workstation or router, for example). The device type can be changed on the Device Properties - General page.
- **Host name**—Displays the DNS name of the device.
- **Address**—Displays the IP address of the device.

The icon associated with the device, over a colored shape that indicates the worst state of any of the active monitors on the device, is displayed to the left of Device Name. The icon can be changed on the Device Properties - General page.

Additional attributes associated with the device (Location, Contact and Description as well as any custom attributes) are displayed below the device icon. Attributes can be added, modified or removed from the Device Properties - Attributes page.

Notes display any additional information associated with the device. Notes are managed on the Device Properties - Notes page.

The following topics give an overview of the device properties available to use and modify:

- General Device Properties, page 2-25
- Device Property Performance Monitors, page 2-26
- Active Monitor Device Properties, page 2-29
- Passive Monitor Device Properties, page 2-29
- Device Property Actions, page 2-29
- Device Property Polling, page 2-30
- Device Property Credentials, page 2-30
- Device Property Notes, page 2-31
- Device Property Custom Links, page 2-31
- Device Property Attributes, page 2-31
- Changing Device Types, page 2-32

General Device Properties

The General section of the Device Properties dialog box provides, and lets you modify, basic information for the selected device.

- **Display name**—An identifying name for the current device. This name is populated during discovery, but can be changed by the user at any time. Changing the name will not change how the device is polled, only how it is displayed in Cisco netManager.
- **Polling type**—Select the type of polling you want Cisco netManager to use for this device.
  - ICMP (TCP/UDP)
  - IPX
  - NetBIOS

  Note If NetBIOS is selected, the Host Name box must contain a valid NetBIOS name. If IPX is selected, the **Address** box must contain a valid IPX address. If NetBIOS or IPX is selected, you cannot monitor TCP/IP services on this device.

- **Poll using**—Select if you want Cisco netManager to use the IP address or the hostname (DNS) of the device for polling.
- **Host name (DNS)**—This should be the official network name of the device if the polling method is ICMP. The network name must be a name that can be resolved to an IP address. If the polling method is NetBIOS or IPX, this must be the NetBIOS or IPX name.
- **Address**—Enter an IP or IPX address.
- **Additional Network Interfaces**—Click this button to configure an additional Network Interface for the current device.

- **Device Type**—Select the appropriate device type from the pull-down menu. The icon displayed will represent the device in all views.

Device Property Performance Monitors

The Performance Monitors section of the Device Properties dialog box lets you configure and manage performance monitors for the selected device. To get to this dialog box, right-click a device from the device list, and select **Properties > Performance Monitor**. For more information, see Chapter 10, "Using Performance Monitors."

Note For some performance monitors, the SNMP credential on the device must be configured. For Windows Management Instrumentation (WMI) performance monitors, the NT credential is required.

If you select a specific performance monitor without configuring the monitor manually, the default collection type is automatically selected. The collection type refers to the item on the current device that is being monitored (this does not pertain to the custom WMI and SNMP monitors that may appear). For Cisco devices all performance monitors, except Interface Utilization and Ping Latency and Availability, will be enabled by default.

The Performance Monitors section of the Device Properties dialog box displays the following options:

- **Enable/Disable Performance Monitors**—check the monitors you want to enable and uncheck monitors you want disabled. Performance monitors will be associated with the device based on its capabilities.

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

Capability	Performance Monitor
Autonomous Access Point	CPU Utilization
	Memory Utilization
	Interface Status
Cisco ASA	Device Inventory Entity Status
	CPU Utilization
	Memory Utilization
	Interface Status
Cisco Unified Communications Manager	Communications Manager Status
	Communications Manager Logical Connectivity
	Device Inventory Entity Status
Cisco Unified Communications Manager Express	Communications Manager Express Status
	Communications Manager Express Logical Connectivity
	Device Inventory Entity Status

Capability	Performance Monitor
Cisco Unity	Cisco Unity Status
	Cisco Unity Port Utilization
	Device Inventory Entity Status
Cisco Unity Connection	Cisco Unity Status
	Cisco Unity Port Utilization
	Device Inventory Entity Status
Cisco Unity Express	Cisco Unity Express Status
	Interface Status
	Device Inventory Entity Status
Cisco PIX Firewall	Device Inventory Entity Status
	CPU Utilization
	Memory Utilization
	Interface Status
Cisco IDS	CPU Utilization
	Memory Utilization
	Interface Status
Cisco IPS	CPU Utilization
	Memory Utilization
	Interface Status
MCS	CPU Utilization
	Memory Utilization
	Disk Utilization
	Temperature Statistics
	Power Supply Status
	Fan Status
	Voice Services Status
	Interface Status
	Device Inventory Entity Status
MPX	Voice Services Status
	Memory Utilization
	Disk Utilization
	CPU Utilization
	Interface Status
	Device Inventory Entity Status

Capability	Performance Monitor
Router	CPU Utilization
	Memory Utilization
	Temperature Statistics
	Interface Status
	Power Supply Status
	Fan Status
	Device Inventory Entity Status
SRST	SRST Status
	Device Inventory Entity Status
Switch	CPU Utilization
	Memory Utilization
	Temperature Statistics
	Interface Status
	Power Supply Status
	Fan Status
	Device Inventory Entity Status
Cisco VPN	Interface Status
Wireless LAN Controller	Wireless LAN Controller Status
	Interface Status
	CPU Utilization
	Memory Utilization

For all other devices, the following performance monitors will be associated:

- CPU Utilization
- Memory Utilization
- Disk Utilization
- Interface Utilization
- Ping Latency and Availability

- **Configure**—Click to configure collection interval (in minutes).

Note If an error occurs, a warning message appears directing you to the problem. If it is a timeout error, you are prompted to open the Advanced dialog box to change the timeout value. For any other error, you are returned to this dialog box.

- **Library**—Click for options to create (New), edit, copy, or delete Performance Monitor Library items to use on all devices.

- **Enable Custom Performance Monitors (for this device only)**—Use this section of the dialog box to add customized Active Script, SNMP, or WMI performance monitors on this device only. The monitors added here do not appear in the Performance Monitor Library, and cannot be used on other devices unless they are manually created for that device.
  - Click **New** to configure a new monitor.
  - Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.
  - Select a performance monitor type, then click **Delete** to remove it from the list.

For information on the Active Script Performance Monitor, please see Adding Custom Performance Monitors to the Performance Monitor Library, page 10-6.

Active Monitor Device Properties

Use the Active Monitors dialog box to display and manage active monitors for a device. To get to this dialog box, right-click a device from the device list, and select **Properties** > **Active Monitor**. Monitors may have been added during initial discovery, when Cisco netManager first added the device to the database

You can do the following from this dialog box:

- Click **Add** to configure a new active monitor.
- Select an active monitor and click **Edit** to change the configuration.
- Select an active monitor and click **Remove** to remove the monitor from the device.

For more information, see Chapter 8, "Using Active Monitors."

Passive Monitor Device Properties

Instead of polling a device, a passive monitor listens for messages and events, then notifies Cisco netManager when they occur.

To configure the passive monitor for a device, right-click a device from the device list, and select **Properties** > **Passive Monitor**. This dialog box displays all passive monitors configured for this device.

You can do the following from this dialog box:

- Click **Add** to configure a new passive monitor.
- Select a passive monitor, then click **Edit** to change the configuration.
- Double-click a passive monitor to edit the configuration.
- Select a passive monitor, then click **Remove** to remove the monitor from the device.

For more information, see Chapter 9, "Using Passive Monitors."

Device Property Actions

You can select an action policy to use on a device or configure alerts specifically for this device. To get to this dialog box, right-click a device from the device list, and select **Properties** > **Actions**.

Select a policy from the Apply this Action Policy pull-down menu. You can also create a new policy or edit an existing action policy by clicking the **Browse** button next to the pull-down menu box.

Configured alerts appear in the Apply individual actions list, displaying the action type that is to be fired and the state change that will trigger the action. You may have multiple actions on a single device.

This dialog box displays all actions configured for this device. You can do the following:

- Click **Add** to configure a new action.
- Select an action, then click **Edit** to change the configuration.
- Double-click an action to edit the configuration.
- Select an action, then click **Remove** to remove the action from the device. Removing the action from the list also deletes all records for this action (on this device) from the action log.

For more information, see Chapter 6, “Using Actions.”

Device Property Credentials

The Credentials dialog box displays Windows and SNMP credentials information for the current device. To get to this dialog box, right-click a device from the device list, and select **Properties** > **Credentials**.

Devices that are SNMP-manageable devices appear on the map view with an icon with a white star in the top right corner.

- **Windows credentials**—Select the Windows credential to connect to this device. Click the Browse (**...**) button to browse the credentials library.
- **SNMPv1/SNMPv2 credentials**—If the Identify devices via SNMP option was selected during discovery or if an SNMP discovery was performed, the correct SNMP credential was used during the discovery process, and if the device is SNMP manageable, then the correct credential is selected automatically. If any of these conditions are not met, None is selected.
- **Device Object ID (OID)**—The SNMP object identifier for the device. This identifier is used to access a device and read other SNMP data.

For more information, see the Configuring Credentials, page 2-12.

Device Property Polling

Polling is the term used for monitoring discovered devices in Cisco netManager. The Polling dialog box lets you configure polling options and schedule maintenance times for the selected device. To get to this dialog box, right-click a device from the device list, and select **Properties** > **Polling**.

- **Poll interval**—This number determines how often Cisco netManager will poll the selected device. Enter the number of seconds you want to pass between polls.
- **Up dependency**—Click to configure additional options, based on when another device is operational, that determine when the selected device is polled.
- **Down dependency**—Click to configure additional options, based on when the selected device is operational, that determine when other devices are polled.
- **Maintenance**—Use this section of the dialog box to manually set the device Maintenance state, or schedule the maintenance state for a certain time period. Any device placed in Maintenance state will not be polled, but it remains in the device list with an identifying icon. By default, the maintenance state is represented by an orange background color.
- **Force this device into maintenance mode now**—Select this option to put the selected device in maintenance mode. Clear the option to resume polling the device.

- **Recurring maintenance times**—This box displays all scheduled maintenance times for the device.
  - Click **Add** to schedule a new maintenance time for the device.
  - Select an entry, then click **Edit** to change a scheduled time.
  - Select an entry, then click **Remove** to delete a scheduled time.

For more information, see Chapter 5, “Polling.”

Device Property Notes

The Notes dialog box provides an option to enter free-form messages into the device database. To get to this dialog box, right-click a device from the device list, and select **Properties** > **Notes**.

The first line of the notes box displays information about when the device was added to the database. If viewing the notes on a shortcut, the date and time the device was added to the database are displayed.

You can customize the notes with any information you want to include about the device. For example, you may want to record historical information about a device, physical location information, or perhaps notes relating to the actions configured for the device.

Device Property Custom Links

In the Cisco netManager web interface, you can use this dialog box to create a custom link for a device.

After a custom link has been configured and added to the Device Status workspace page, it appears in the Device Custom Links report on the Device Status page for the selected device.

You can do the following from this dialog box:

- Click **Add** to add a new custom link.
- Select a custom link in the list, then click **Edit** to change the settings.
- Select a custom link in the list, then click **Remove** to remove it from the list.

Note Custom links created in the web interface are not visible in the console. Menu items configured in the console are not visible in the web interface.

Device Property Attributes

The Attributes dialog box lists attributes that are associated with a device, such as contact person, location, serial number, etc. To get to this dialog box, right-click a device from the device list, and select **Properties** > **Attributes**. The first attributes in the list are added by Cisco netManager when the device is added to the database, either by the Device Discovery wizard, or through another means.

You can do the following from this dialog box:

- Click **Add** to add a new device attribute. The Add Attribute dialog box opens.
- Select a device attribute in the list, then click **Edit** to change the settings.
- Select a device attribute in the list, then click **Remove** to remove it from the list.

Changing Device Types

Device Types act like templates for new devices, containing device properties (such as active and passive monitors, menu items, etc.) and represented by different icons in Device Properties.

When you change a device type on an existing device, you are only changing the icon that represents the device, and not adding additional information and settings to the device. If you rediscover the device, the icon will change back to the original device type. All other changes will have to be done manually.

To change a device type icon on an existing device:

Step 1 In Device view, right-click a device. In the context menu, click **Properties** > **General**.

Step 2 In the Device type list, select a new device type.

Step 3 Click **OK** to save changes.

Editing Multiple Devices with Bulk Field Change

The Bulk Field Change feature gives you the ability to make changes to multiple devices and device groups. You must have administrative privileges to the devices or device groups that you want to make changes to.

Step 1 Select the devices or device groups you want to change, then right-click and select **Bulk Field Change**. The Bulk Field Change context menu opens.

Note When you select a device group, every device in the group, and any subgroup of the group, will reflect the bulk field change.

Step 2 Select the field you want to change. The following items can be modified through Bulk Field Change:

- Credentials
- Polling Interval
- Maintenance Mode
- Maintenance Schedule (web interface only)
- Device Type
- Action Policy
- Up Dependency
- Down Dependency
- Notes
- Attribute
- Performance Monitors
- Active Monitor
- Active Monitor Properties
- Passive Monitor (web interface only)

- Passive Monitor Properties (web interface only)

Step 3 Enter the configuration information that you want to set.

Step 4 Click **OK** to save changes.

Using Acknowledgements

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. The device name appears in bold in the Device List.

After the device is in Acknowledgement mode, it will remain so until you actively acknowledge it.

Note Acknowledging a device state change does not keep that device from firing actions. To stop a device from firing actions, you must put the device into Maintenance state.

To acknowledge a state change, select the device or devices you want to acknowledge, right-click, then click **Acknowledge Events**. For a list of events, see Appendix A, “Events Processed.”

CHAPTER 3

Understanding Workspaces and Workspace Content

Workspaces contain multiple *views* that let you organize workspace content by the type of information they display. When you begin customizing your workspace views, you should consider the types of information you need to view most often, the devices to which you need to pay closest attention, and the level of detail you want to monitor through a particular workspace view. You should also take into consideration the type of workspace, and the types of workspace content you can add. For more information on workspace content, see About Workspace Content, page 3-7.

About Workspaces

Cisco netManager comes with two workspaces:

- **Home workspace**. This is the first screen you see after you log in to the web interface. This universal workspace is designed to house the network information that you typically need. The default Home workspace view cannot be customized, but you can make a copy of it and then add different types of workspace content. For more information on workspace content, see About Workspace Content, page 3-7.
- **Device Status workspace**. This workspace is limited to display only device-level workspace content. Only workspace content specific to a single device can be placed on a device status workspace. When you change the device-in-context, the workspace contents displayed show data corresponding to the newly selected device.

  To access the Device Status workspace, select the Device Tab and double-click a device.

Note For changes that you make in workspace views under your account, your user account will be the only account affected by these changes.

Home Workspace

The Cisco netManager Home workspace is the first screen that you see after you log in to the web interface. This universal workspace is designed to display the network information that you typically need.

The Home Workspace contains preconfigured views:

- Home Page View

- Problem Areas 1 and Problem Areas 2.

Home Page View

The Home Page view cannot be customized, but you can make a copy of it and then add different types of workspace content. It displays typical information about the monitored devices in your network. Specific to the Home Workspace and also on the Home Page view are the following workspace contents:

- **Monitoring Dashboard**—Launches topology views and the device list, which displays events.
- **Device and Phone Summary**—Displays a summary of the number of devices and phones that are reachable. Device status can have one of the following values:

  Devices

  - **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.

  Phones

  - **Registered**—Phones registered with a Cisco Unified Communications Manager.
  - **Unregistered**—Phones not registered with a Cisco Unified Communications Manager.

Note The Phones Summary will appear only if you have the appropriate license. The ability to view and monitor Unified Communication devices depends upon the type of licensing you have.

- **Ping - Devices with Ping Availability under 50%**—Displays devices with ping availability percentages below 50%.

Problem Areas 1 and Problem Areas 2

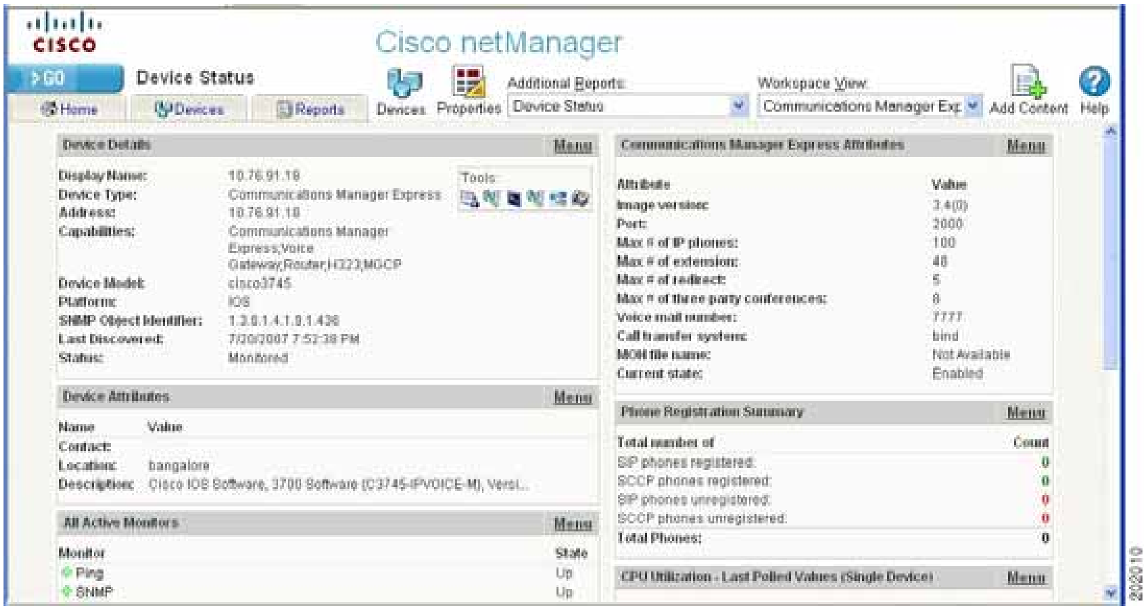
Problem Areas 1 and Problem Areas 2 are views that you can decide to keep, alter, expand, or remove. Each page has default workspace content that provides you with troubleshooting information.

For more information on workspace content, see About Workspace Content, page 3-7 You can also create your own workspace views for the Home Workspace through the Manage Workspace Views dialog box. For more information, see Managing Workspace Views, page 3-4.

Device Status Workspace

The Device Status workspace displays device details for a network device. To access the Device Status workspace, select the Device Tab and double-click a device. You can change the device-in-context, but the workspace content in each workspace view remains the same. Only workspace content specific to a single device can be placed on a device status workspace. For more information on what types of device workspace content is available, see Device Workspace Content, page 3-11.

Figure 3-1 Device Status Workspace



Device Status

Additional Reports: Device Status

Workspace View: Communications Manager Exp

Device Details Menu

Display Name:	10.76.91.18
Device Type:	Communications Manager Express
Address:	10.76.91.18
Capabilities:	Communications Manager Express,Voice Gateway,Router,H323,MGCP
Device Model:	cisco3745
Platform:	IOS
SNMP Object Identifier:	1.3.6.1.4.1.9.1.436
Last Discovered:	7/20/2007 7:52:38 PM
Status:	Monitored

Device Attributes Menu

Name	Value
Contact:	
Location:	bangalore
Description:	Cisco IOS Software, 3700 Software (C3745-IPVOICE-M), Versi...

All Active Monitors Menu

Monitor	State
Ping	Up
SNMP	Up

Communications Manager Express Attributes Menu

Attribute	Value
Image version:	3.4(0)
Port:	2000
Max # of IP phones:	100
Max # of extension:	48
Max # of redirect:	5
Max # of three party conferences:	8
Voice mail number:	7777
Call transfer system:	bind
MOH file name:	Not Available
Current state:	Enabled

Phone Registration Summary Menu

Total number of	Count
SIP phones registered:	0
SCCP phones registered:	0
SIP phones unregistered:	0
SCCP phones unregistered:	0
Total Phones:	0

CPU Utilization - Last Polled Values (Single Device) Menu

Figure 3-1 shows an example of a Device Status workspace. The Devices icon opens the Devices Tab and the Properties icon opens the property attributes for the selected device.

The Device Status workspace has several preconfigured workspace views:

- Device-specific workspace (Cisco Unified Communications Manager, Cisco Unity, and so on.)
- Disk/CPU/Memory
- General
- Problem Areas

You can view full device reports by selecting a report from the More Device Reports drop-down list. For more information on Device Reports, see About Device Reports, page 11-3.

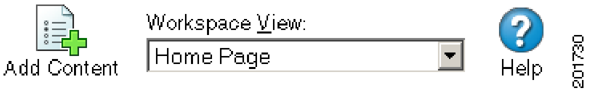
Note If workspace content or report information is not relevant or available for a selected device, the workspace content or report will show no data.

Workspace Toolbar

The Workspace Toolbar provides links for accessing the Cisco netManager workspaces, and tools for managing workspace views and content.

Figure 3-2 shows an example of the Workspace Toolbar.

Figure 3-2 Workspace Toolbar



Workspace View: Home Page

The following options are available:

- **Add Content.** Use this button to add workspace content to your workspace views.
- **Workspace View.** Use this drop-down menu to edit your workspace views and to switch between workspace views.
- **Help.** Use this button to view the Cisco netManager Help for the window you are currently viewing.

Managing Workspace Views

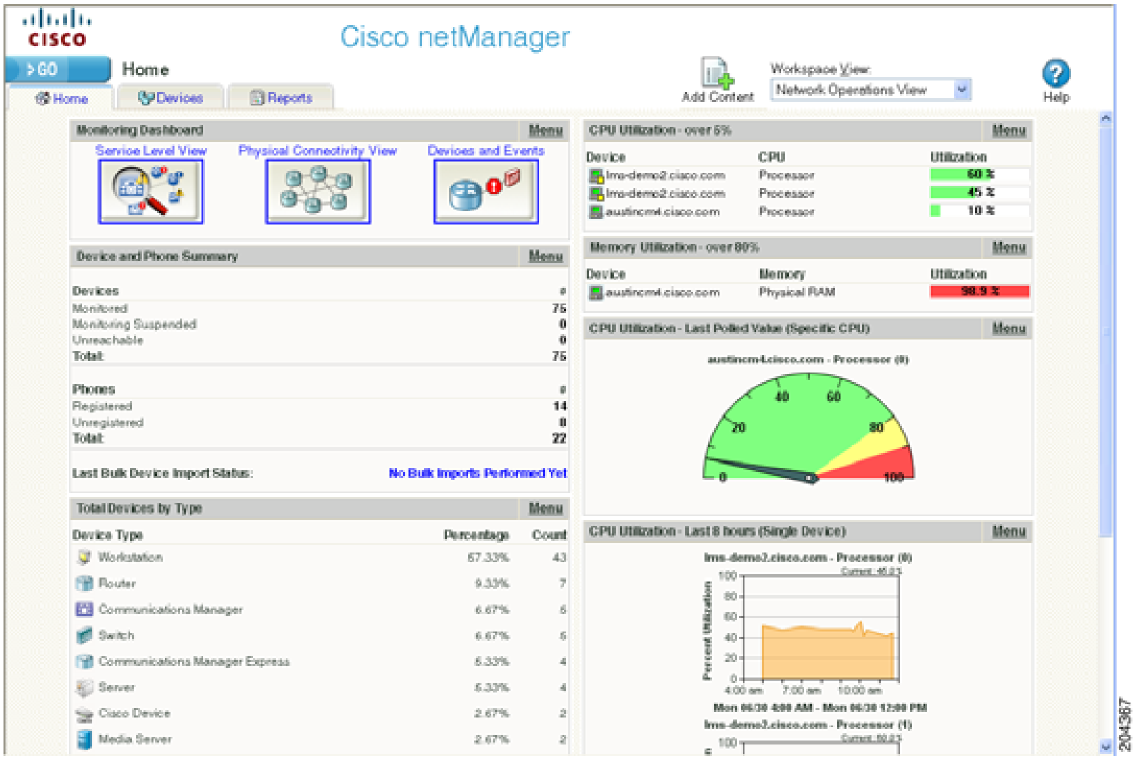
You can create more of your own workspace views to use along with the preconfigured views. You can create as many as you feel are necessary to organize your system for efficient reporting. You can also edit these views as needed:

- From the Workspace View drop-down menu, select **Manage Workspace Views**.
- Select **GO > Configure > Manage Workspace Views**.

In the Manage Workspace Views dialog, you can create new workspace views, and edit, copy, or delete an existing workspace view.

- Click **New** to configure a new workspace. Figure 3-3 shows an example of a customized view that a user named Network Operations View.
- Select an existing workspace view and click **Edit** to change the current configuration of a workspace.
- Double-click an existing workspace to change its configuration.
- Select a workspace view, then click **Copy** to make a copy of that workspace and add it to the list.
- Select a workspace view, then click **Copy to** to copy an existing workspace to another user.
- Select a workspace monitor view, then click **Delete** to remove it from the list.

Figure 3-3 Customized Workspace Example



Devices	#
Monitored	75
Monitoring Suspended	0
Unreachable	0
Total:	75

Phones	#
Registered	14
Unregistered	8
Total:	22

Last Bulk Device Import Status: No Bulk Imports Performed Yet

Device Type	Percentage	Count
Workstation	57.33%	43
Router	9.33%	7
Communications Manager	6.67%	5
Switch	6.67%	5
Communications Manager Express	5.33%	4
Server	5.33%	4
Cisco Device	2.67%	2
Media Server	2.67%	2

Device	CPU	Utilization
lms-demo2.cisco.com	Processor	60 %
lms-demo2.cisco.com	Processor	45 %
austincm4.cisco.com	Processor	10 %

Device	Memory	Utilization
austincm4.cisco.com	Physical RAM	98.9 %

Creating a New Workspace View

Step 1 From the Manage Workspace Views dialog, select **New**. The New Workspace View dialog opens.

Enter the appropriate information in the following fields:

- **View name.** Enter a name for the workspace view.
- **View type.** Choose a type for the workspace view from the drop-down menu.
- **Column count.** Enter a value for the number of columns you wish to have in the new workspace view. Keep in mind that the more columns you include, the smaller the data displayed inside a workspace.
- Enter a value in pixels for each of the workspace columns.

Step 2 Click **OK** to save changes.

Editing a Workspace View

To edit a workspace view:

Step 1 From the Manage Workspace Views dialog, select **Edit**. The Edit Workspace View dialog opens.

Step 2 Enter the appropriate information in the following fields:

- **Workspace name.** The workspace title as it appears in the Workspace Library.
- **Workspace type.** The workspace type as it appears in the Workspace Library (Home or Device).

Note Workspace view types cannot be edited after a view is created.

- **Column count.** The number of columns in the workspace.
- **Column width.** The width of each column in the workspace, in pixels.

Step 3 Click **OK** to save changes.

To copy an existing workspace view:

Step 1 From the Manage Workspace Views dialog, select **Copy**. The Edit Workspace View dialog opens.

Enter the appropriate information in the following fields:

- **Workspace name.** The workspace title as it appears in the Workspace Library.
- **Column count.** The number of columns in the workspace.
- **Column width.** The width of each column in the workspace in pixels.

Step 2 Click **OK** to save changes.

To copy a workspace view to another Cisco netManager user:

Step 1 From the Manage Workspace Views dialog, select **Copy to**. The Edit Workspace View dialog opens.

Enter the appropriate information into the following fields:

- **Copy to user**. From the drop-down menu, select a user account in which to copy the workspace view.
- **View name**. The name of the workspace view as it will appear in the Workspace Library.

Step 2 Click **OK** to save.

Deleting a Workspace View

To delete a workspace view:

Step 1 From the Manage Workspace Views dialog, click **Delete**.

Step 2 Click **OK** on the dialog that follows.

Navigating Through Workspaces

The main way to navigate from one workspace view to another is through the Workspace toolbar. From here you can add content to a workspace, manage your workspace and workspace views, and access the Cisco netManager help system.

Workspace Toolbar

- **Add Content—**Use this button to add workspace content to your workspace views.
- **Workspace View**—Use this drop-down list to edit and switch between workspace views.
- **Help**—Use this button to view the Cisco netManager Help for the window you are currently viewing.

About Workspace Content

Workspace content is a quick view of a report. Cisco netManager offers a collection of more than 100 configurable types of workspace content for display in workspace views. Workspace content shows information that is similar to the information found in reports. However, workspace content is not interactive, but only displays data. Workspace content shows a quick view of a report. For more information about reports, see Chapter 11, "Using Reports."

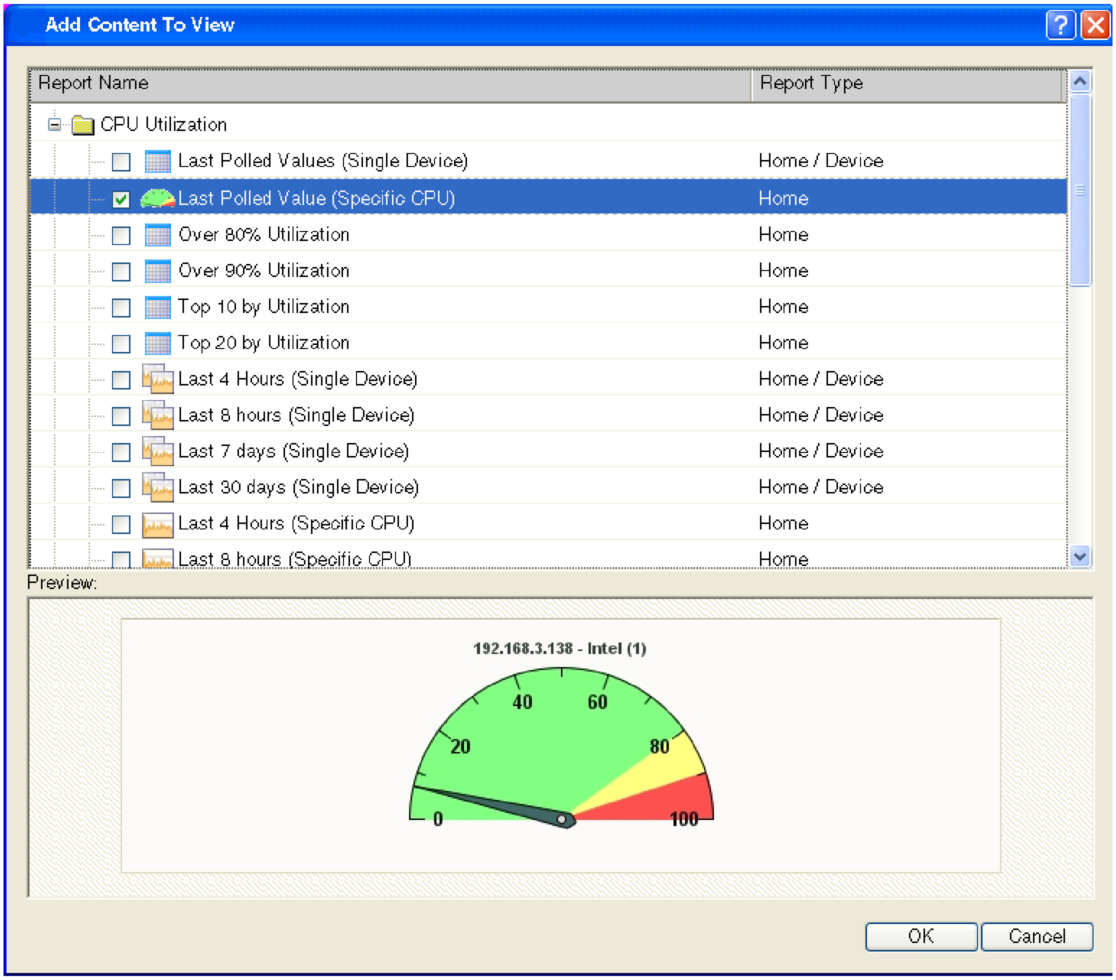
Note If workspace content or report information is not relevant or available for a selected device, the workspace content or report will show no data.

You can do the following to workspace content in a workspace view:

- To add content, click **Add content** on the Workspace Toolbar. On the Add content to view dialog, you can select multiple types of workspace content, from multiple categories. A preview for the workspace content is displayed at the bottom of the dialog.
- To remove content, go to the menu for that workspace content and select **Close**. Keep in mind that when you remove content, any customizations you have made to it are lost.
- To move workspace content, click its title bar and drag it to a new space in the workspace view.

You can customize a workspace by adding additional workspace contents to a workspace view. To add workspace content to a workspace view:

Step 1 In the Workspace toolbar, click **Add Content**. The Add Content To View page opens.



Report Name	Report Type
⊟ CPU Utilization	
□ Last Polled Values (Single Device)	Home / Device
☑ Last Polled Value (Specific CPU)	Home
□ Over 80% Utilization	Home
□ Over 90% Utilization	Home
□ Top 10 by Utilization	Home
□ Top 20 by Utilization	Home
□ Last 4 Hours (Single Device)	Home / Device
□ Last 8 hours (Single Device)	Home / Device
□ Last 7 days (Single Device)	Home / Device
□ Last 30 days (Single Device)	Home / Device
□ Last 4 Hours (Specific CPU)	Home
□ Last 8 hours (Specific CPU)	Home

Step 2 Click the **plus symbol (+)** button next to a workspace content category folder, then click to select the workspace content you want to add to the workspace view.

Step 3 Click **OK** to save changes. The new workspace content is added to the workspace view.

Workspace Content Categories

Workspace content is categorized according to the type of information it displays:

- **CPU Utilization**—Displays information pertaining to device and network CPU levels.
- **Custom Performance Monitors**—Displays information pertaining to your custom performance monitors.
- **Device**—Available from the Device Status Workspace. Displays workspace content specific to a single device that is selected from the Device tab. When you change the device-in-context, the content shows data corresponding to the newly selected device.
- **Disk Utilization**—Displays information pertaining to device and network disk levels.
- **Fan Status**—Displays fan status with the last polled time stamp.

- **General**—Displays information on your Cisco netManager settings and diagnostics, as well as device-specific and user-configured details.
- **HomePage—**Available from the HomeSpace Workspace. Displays a summary of device states, devices with ping availability percentages below 50%, and a monitoring dashboard where you can launch topology views and device events of your network.
- **Interface Utilization**—Displays information pertaining to device and network interfaces.
- **Inventory**—Displays network devices and their settings, including actions, monitors, and policies.
- **Memory Utilization**—Displays information pertaining to device and network memory levels.
- **Performance**—Displays information gathered from WMI and SNMP Performance Monitors, regarding your network devices' CPU, disk, interface, and memory utilization; and ping latency and availability.
- **Ping Availability and Response Time**—Displays information pertaining to device ping availability, response time, and packet loss.
- **Power Supply Status**—Displays the device’s power supply status with the last polled timestamp.
- **Problem Areas**—Displays troubleshooting content that allows you to investigate network issues.
- **Temperature Status**—Displays the device’s temperature status with the last polled timestamp.
- **Threshold**—Displays information on your network's CPU, disk, interface, and memory utilization; also displays ping function; at or above a specific threshold.
- **Top 10**—Displays the top devices on your network according to their CPU, disk, interface, and memory utilization; also displays ping function.

Workspace content is listed multiple times on the Add Content dialog box. For example, Disk Utilization is listed under Disk Utilization, Threshold, Top 10, and Performance categories.

Workspace Content Types

The following are the workspace content types available in Cisco netManager:

(H) = Home

(D) = Device

CPU Utilization Workspace Content

Table 3-1 CPU Utilization Workspace Content

Content	Description
(H) Last Polled Values (specific CPU)	Shows the CPU utilization for a specific device CPU at the time of the last poll.
(H) All CPUs over 80% Utilization	Lists all network devices with a CPU utilization greater than 80%.
(H) All CPUs over 90% Utilization	Lists all network devices with a CPU utilization greater than 90%.
(H) Top 10 CPUs by Utilization	Lists the top 10 devices based on their current CPU utilization percentage.
(H) Top 20 CPUs by Utilization	Lists the top 20 devices based on their current CPU utilization percentage.

Table 3-1 CPU Utilization Workspace Content (continued)

Content	Description
(D) Last 4 hours CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 4 hours.
(D) Last 8 hours CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 8 hours.
(D) Last 7 days CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 7 days.
(D) Last 30 days CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 30 days.
(H) Last 4 hours CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device over the last 4 hours.
(H) Last 8 hours CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device over the last 8 hours.
(H) Last 7 days CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device over the last 7 days.
(H) Last 30 days CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device of the last 30 days.

Custom Performance Monitor Workspace Content

Table 3-2 Custom Performance Monitor Workspace Content

Content	Description
(H) Last Polled Value (specific monitor)	Details information on a specific custom performance monitor at the time of the last poll.
(H) Top 10 with threshold	Lists the top 10 devices by a custom performance monitor threshold.
(H) Top 20 with threshold	Lists the top 20 devices by a custom performance monitor threshold.
(H) Top 20 by specific monitors	Lists the top 20 devices by a specific custom performance monitor.
(D) Last 4 hours (single device)	Details a device's custom performance monitors over the last 4 hours.
(D) Last 8 hours (single device)	Details a device's custom performance monitors over the last 8 hours.
(D) Last 7 days (single device)	Details a device's custom performance monitors over the last 7 days.
(D) Last 30 days (single device)	Details a device's custom performance monitors over the last 30 days.
(H) Last 4 hours (specific monitor)	Details a specific custom performance monitor over the last 4 hours.
(H) Last 8 hours (specific monitor)	Details a specific custom performance monitor over the last 8 hours.

Table 3-2 Custom Performance Monitor Workspace Content (continued)

Content	Description
(H) Last 7 days (specific monitor)	Details a specific custom performance monitor over the last 7 days.
(H) Last 30 days (specific monitor)	Details a specific custom performance monitor over the last 30 days.

Device Workspace Content

Table 3-3 Device Workspace Content

Content	Description
Device chassis summary	Displays description and manufacturer name of chassis.
Flash Devices summary	Displays description, index, and size of flash devices.
Flash Files summary	Displays the names of flash files on the device.
Interface summary	Displays the description of an interface and its administrative and operational status.
Module summary	Displays description and operational status of modules.
Phone registration summary	Displays the number of Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP) phones that are registered to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.
Software Image Information	Displays various details of the software image on the device.
Stack Summary	Displays description and manufacturer name of stack.
Cisco Unified Communications Manager attributes	Displays attributes specific to the Cisco Unified Communications Manager, including hostname, description, software version, cluster ID and status.
Cisco Unified Communications Manager Express attributes	Displays attributes specific to the Cisco Unified Communications Manager Express.
Unity port summary	Displays the phone system on each port and its status.
Unity attributes	Displays the version of Cisco Unity on the device and the number of active, active inbound, outbound, and outbound active ports.
Unity Express attributes	Displays attributes specific to the Cisco Unity Express.
Voice gateway registration summary	Displays number of voice gateways registered with a Cisco Unified Communications Manager.
Voice services summary	Displays the status of all voice services associated with this device.
Wireless LWAP channel utilization	Displays a list of interfaces on the access points and their channel utilization.
Wireless LWAP summary	Displays names of lightweight access points and the operational status for a wireless LAN controller.

Disk Utilization Workspace Content

Table 3-4 Disk Utilization Workspace Content

Content	Description
(D) Last Polled Values (single device)	Shows the disk utilization for all of a device's disks at the time of the last poll.
(H) Last Polled Values (specific disk)	Shows the disk utilization for a specific device disk at the time of the last poll.
(H) All Disks Over 80%	Lists all network devices with a disk utilization greater than 80%.
(H) All Disks Over 90%	Lists all network devices with a disk utilization greater than 90%.
(H) Top 10 Disks by Percent Utilization	Lists the top 10 devices based on their current disk utilization percentage.
(H) Top 20 Disks by Percent Utilization	Lists the top 20 devices based on their current disk utilization percentage.
(H) Top 10 Disks by Free Space	Lists the top 10 devices based on their current free disk space.
(H) Top 20 Disks by Free Space	Lists the top 20 devices based on their current free disk space.
(D) Last 4 hours Disk Utilization (single device)	Details all disk utilization percentages for one device over the last 4 hours.
(D) Last 8 hours Disk Utilization (single device)	Details all disk utilization percentages for one device over the last 8 hours.
(D) Last 7 days Disk Utilization (single device)	Details all disk utilization percentages for one device over the last 7 days.
(D) Last 30 days Disk Utilization (single device)	Details all disk utilization percentages for one device over the last 30 days.
(H) Last 4 hours Disk Utilization (single device)	Details a specific disk's utilization percentages for one device over the last 4 hours.
(H) Last 8 hours Disk Utilization (specific disk)	Details a specific disk's utilization percentages for one device over the last 8 hours.
(H) Last 7 days Disk Utilization (specific disk)	Details a specific disk's utilization percentages for one device over the last 7 days.
(H) Last 30 days Disk Utilization (specific disk)	Details a specific disk's utilization percentages for one device over the last 30 days.
(H) Last 4 hours Disk Free Space (specific disk)	Details a specific disk's free space for one device over the last 4 hours.
(H) Last 8 hours Disk Free Space (specific disk)	Details a specific disk's free space for one device over the last 8 hours.
(H) Last 7 days Disk Free Space (specific disk)	Details a specific disk's free space for one device over the last 7 days.
(H) Last 30 days Disk Free Space (specific disk)	Details a specific disk's free space for one device over the last 30 days.

Fan Status

The Fan Status report displays the fan status on the device with the last polled timestamp.

General Workspace Content

Table 3-5 General Workspace Content

Contents	Description
(D) Device Attributes	Displays a device's attributes configured in **Device Properties > Attributes**.
(D) Device SNMP Details	Displays a device's SNMP details.
(D) Device Details	Displays a device's details configured in **Device Properties > General**.
(D) Device Custom Links	Displays any custom links assigned to a device in **Device Properties > Custom Links**.
(D) Device Dependencies	Shows the state of a device and any devices that are up or down dependent on that device.
(D) Device Active Monitor States	Lists all of a device's active monitors and their current state.
(D) Performance Monitor Summary	Displays a polling summary for the device-in-context.
(H) Map View	Displays a smaller version of a network map.
(H) Database Size	Displays a graphical representation of the Cisco netManager database at the time of the last poll.
(H) Custom Links	Displays any custom links that you add to the workspace.
(H) Free Form Text/HTML	Displays any free-form text or HTML code that you add to the workspace.
(H) Web User Activity Log	Displays a log of when a user logs in or out of the web interface, and the actions taken while logged in.
(H) Interface Details	Displays SNMP information reported by a specific network interface.
(H) User Orientation	Displays information regarding the workspaces, and workspace content.

Interface Utilization Workspace Content

Table 3-6 Interface Utilization Workspace Content

Contents	Description
(D) Last Polled Interface (single device)	Shows the interface utilization for all network interfaces at the time of the last poll.
(H) Last Polled Interface (specific interface)	Shows the interface utilization for a specific network interface at the time of the last poll.
(H) All Interfaces over 80% Bandwidth Utilization	Lists all network interfaces with a utilization greater than 80%.

Table 3-6 Interface Utilization Workspace Content (continued)

Contents	Description
(H) All Interfaces over 90% Bandwidth Utilization	Lists all network interfaces with a utilization greater than 90%.
(H) Top 10 Devices by Bandwidth Utilization	Lists the top 10 devices based on their current interface utilization.
(H) Top 20 Devices by Bandwidth Utilization	Lists the top 20 devices based on their current interface utilization.
(H) Top 10 Devices by Interface Traffic	Lists the top 10 devices based on their current interface traffic.
(H) Top 20 Devices by Interface Traffic	Lists the top 20 devices based on their current interface traffic.
(D) Last 4 hours Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 4 hours.
(D) Last 8 hours Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 8 hours.
(D) Last 7 days Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 7 days.
(D) Last 30 days Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 30 days.
(H) Last 4 hours Interface Utilization (specific interface)	Details a specific interface's utilization for one device over the last 4 hours.
(H) Last 8 hours Interface Utilization (single device)	Details a specific interface's utilization for one device over the last 8 hours.
(H) Last 7 days Interface Utilization (specific interface utilization)	Details a specific interface's utilization for one device over the last 7 days.
(H) Last 30 days Interface Utilization (specific interface utilization)	Details a specific interface's utilization for one device over the last 30 days.

Inventory Workspace Content

Table 3-7 Inventory Workspace Content

Contents	Description
(H) Total Devices by Type	Lists all monitored network devices by type and number.
(H) Total Active Monitors by Type	Lists all active monitors on the network by type and number.
(H) Total Passive Monitors by Type	Lists all passive monitors on the network by type and number.
(H) Total Performance Monitors by Type	Lists all performance monitors on the network by type and number.
(H) Total Actions Applied by Type	Lists all actions on the network by type and number.

Table 3-7 Inventory Workspace Content

Contents	Description
(H) Total Devices with Specific Attributes	Lists all devices with a specific attribute.
(H) Active Discovery Results	Once an active discovery is performed, the results are listed here.

Memory Utilization Workspace Content

Table 3-8 Memory Utilization Workspace Content

Contents	Description
(D) Last Polled Memory Utilization (single device)	Shows the memory utilization for all of a device's memory at the time of the last poll.
(H) Last Polled Memory Utilization (specific aspect)	Shows the memory utilization for a specific network device at the time of the last poll.
(H) All Memories over 80% Utilization	Lists all network devices with a memory utilization greater than 80%.
(H) All Memories over 90% Utilization	Lists all network devices with a memory utilization greater than 90%.
(H) Top 10 Devices by Memory Utilization	Lists the top 10 devices based on their current memory utilization.
(H) Top 20 Devices by Memory Utilization	Lists the top 20 devices based on their current memory utilization.
(D) Last 4 hours Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 4 hours.
(D) Last 8 hours Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 8 hours.
(D) Last 7 days Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 7 days.
(D) Last 30 days Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 30 days.
(H) Last 4 hours Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 4 hours.
(H) Last 8 hours Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 8 hours.
(H) Last 7 days Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 7 days.
(H) Last 30 days Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 30 days.

Performance - Historic Workspace Content

Table 3-9 Performance - Historic Workspace Content

Contents	Description
(D) Custom Performance Monitor Values (last 4 hours - single device)	Details a device's custom Performance Monitor values over the last 4 hours.
(D) Interface Utilization (last 4 hours - single device)	Details all interface utilization percentages for one device over the last 4 hours.
(D) CPU Utilization (last 4 hours - single device)	Details all CPU utilization percentages for one device over the last 4 hours.
(D) Memory Utilization (last 4 hours - single device)	Details all memory utilization percentages for one device over the last 4 hours.
(D) Disk Utilization (last 4 hours - single device)	Details all disk utilization percentages for one device over the last 4 hours.
(D) Ping Response Time (last 4 hours - single device)	Details all ping response times for device's interfaces over the last 4 hours.
(D) Ping Availability (last 4 hours - single device)	Details all ping availability for a device's interfaces over the last 4 hours.
(H) Interface Traffic (last 4 hours - specific interface)	Details interface traffic for a specific device interface over the last 4 hours.
(H) Custom Performance Monitor Values (last 4 hours - specific monitor)	Details a device's specific custom Performance Monitor values over the last 4 hours.
(H) Interface Utilization (last 4 hours - specific interface)	Details a specific interface's utilization percentages for one device over the last 4 hours.
(H) CPU Utilization (last 4 hours - specific CPU)	Details a specific CPU's utilization percentages for one device over the last 4 hours.
(H) Memory Utilization (last 4 hours - specific memory)	Details a specific memory's utilization percentages for one device over the last 4 hours.
(H) Disk Utilization (last 4 hours - specific disk)	Details a specific disk's utilization percentages for one device over the last 4 hours.

Performance - Last Poll Workspace Content

Table 3-10 Performance - Last Poll Workspace Content

Contents	Descriptions
(D) Custom Performance Monitor Values (single device)	Shows the values for all of a device's custom Performance Monitors at the time of the last poll.
(D) Interface Utilization (single device)	Shows the interface utilization for all of a device's interfaces at the time of the last poll.
(D) CPU Utilization (single device)	Shows the CPU utilization for all of device's CPUs at the time of the last poll.

Table 3-10 Performance - Last Poll Workspace Content (continued)

Contents	Descriptions
(D) Memory Utilization (single device)	Shows the memory utilization for all of a device's memory at the time of the last poll.
(D) Disk Utilization (single device)	Shows the disk utilization for all of a device's disks at the time of the last poll.
(H) Custom Performance Monitor Values (specific monitor)	Shows the values for a specific device custom Performance Monitor.
(H) Interface Utilization (specific interface)	Shows the utilization of a specific device interface at the time of the last poll.
(H) CPU Utilization (specific CPU)	Shows the utilization of a specific device CPU at the time of the last poll.
(H) Memory Utilization (specific aspect)	Shows the utilization of a specific device memory at the time of the last poll.
(H) Disk Utilization (specific disk)	Shows the utilization of a specific device disk at the time of the last poll.
(H) Ping Response Time (specific interface)	Shows the ping response time of a specific device interface at the time of the last poll.

Ping Availability and Response Time Workspace Content

Table 3-11 Ping Availability and Response Time Workspace Content

Contents	Description
(D) Last 4 hours (single device)	Shows the ping response time for all of a device's interfaces over the last 4 hours.
(D) Last 8 hours (single device)	Shows the ping response time for all of a device's interfaces over the last 8 hours.
(D) Last 7 days (single device)	Shows the ping response time for all of a device's interfaces over the last 7 days.
(D) Last 30 days (single device)	Shows the ping response time for all of a device's interfaces over the last 30 days.
(D) Last 4 hours (single device)	Shows the ping availability for all of a device's interfaces over the last 4 hours.
(D) Last 8 hours (single device)	Shows the ping availability for all of a device's interfaces over the last 8 hours.
(D) Last 7 days (single device)	Shows the ping availability for all of a device's interfaces over the last 7 days.
(D) Last 30 days (single device)	Shows the ping availability for all of a device's interfaces over the last 30 days.
(H) Last Polled Response Time (specific interface)	Shows the last ping response time of a specific device interface at the time of the last poll.
(H) Top 10 by Ping Response Time	Lists the top 10 devices based on their current ping response time.

Table 3-11 Ping Availability and Response Time Workspace Content (continued)

Contents	Description
(H) Top 20 by Ping Response Time	Lists the top 20 devices based on their current ping response time.
(H) Top 10 by Ping Packet Loss	Lists the top 10 devices based on their current ping packet loss.
(H) Top 20 by Ping Packet Loss	Lists the top 20 devices based on their current ping packet loss.
(H) Devices with Ping Response Time over 100 msec	Lists all devices with a ping response time greater than 100 msec.
(H) Devices with Ping Response Time over 500 msec	Lists all devices with a ping response time greater than 500 msec.
(H) Devices with Ping Packet Loss over 50%	Lists all devices with a ping packet loss greater than 50%.
(H) Devices with Ping Packet Loss over 75%	Lists all devices with a ping packet loss greater than 75%.
(H) Devices with Ping Availability over 75%	Lists all devices with a ping availability greater than 75%.

Power Supply Status

This report displays the device’s power supply status with the last polled timestamp.

Problem Areas Workspace Content

Table 3-12 Problem Areas Workspace Content

Contents	Description
(D) Devices with Down Active Monitors	Displays a device's down active monitors.
(D) All Down Interfaces	Displays a device's down interfaces.
(D) Tail of State Change Log	Displays the tail (last 10 records) of the State Change Log for a specified device.
(D) Tail of Syslog	Displays the tail (last 10 records) of the Syslog full report for a specified device.
(D) Tail of Windows Event Log	Displays the tail (last 10 records) of the Windows Event Log for a specified device.
(D) Tail of SNMP Trap Log	Displays the tail (last 10 records) of the SNMP Trap Log for a specified device.
(D) Tail of Action Activity Log	Displays the tail (last 10 records) of the Action Activity Log for a specified device.
(D) Tail of Passive Monitor Error Log	Displays the tail (last 10 records) of the Passive Monitor Error Log for a specified device.
(D) Web Alarms	Displays any web alarms fired for a specified device.
(D) Tail of Device Events	Displays the tail (last 10 records) of the Event Log for a specified device.

Table 3-12 Problem Areas Workspace Content (continued)

Contents	Description
(H) All Completely Down Devices	Displays down devices for a specified device group.
(H) All Down Interfaces	Displays down interfaces for a specified device group.
(H) Devices with Down Active Monitors	Displays devices with down active monitors within a specified device group.
(H) Unacknowledged Devices	Displays unacknowledged devices within a specified device group.
(H) Devices that have fired an Action in the last X hours	Displays devices that have fired an action over the selected time period.
(H) Tail of State Change Log	Displays a tail of the State Change Log for your network.
(H) Summary Counts	Displays a summary of a specified device group.
(H) Tail of Syslog	Displays the tail of the Syslog full report for your network.
(H) Tail of Windows Event Log	Displays the tail of the Windows Event Log for your network.
(H) Tail of SNMP Trap Log	Displays the tail of the SNMP Trap Log for your network.
(H) Tail of Action Activity Log	Displays the tail of the Action Activity Log for your network.
(H) Tail of Passive Monitor Error Log	Displays the tail of the Passive Monitor Error Log for your network.
(H) Map View	Displays a smaller version of a network map.
(H) Device Group Mini Status	Lists all devices in a device group and displays their status by color.
(H) Web Alarms	Shows a snapshot of the most recent web alarms fired on your network.
(H) General Error Log	Displays the tail of the General Error Log for your network.

Temperature Status

This workspace content displays the device’s temperature status with the last polled timestamp. The temperature sensor name is a hyperlink that will take you to the Temperature Statistics report.

Threshold Workspace Content

Table 3-13 Threshold Workspace Content

Contents	Description
(H) Ping Response Time	Displays the top devices based on their current ping response time thresholds.
(H) Ping Packet Loss	Displays the top devices based on their current ping packet loss thresholds.
(H) CPU Utilization	Displays the top devices based on their current CPU utilization percentage thresholds.
(H) Memory Utilization	Displays the top devices based on their current memory utilization percentage thresholds.

Table 3-13 Threshold Workspace Content (continued)

(H) Disk Utilization	Displays the top devices based on their current disk utilization percentage thresholds.
(H) Disk Free Space	Displays the top devices based on their current disk free space thresholds.
(H) Interface Utilization	Displays the top devices based on their current interface utilization percentage thresholds.
(H) Interface Traffic	Displays the top devices based on their current interface traffic thresholds.
(H) Custom WMI/SNMP	Displays the top devices based on their current custom WMI/SNMP thresholds.
(H) Ping Availability	Displays the top devices based on their current ping availability thresholds.

Configuring Threshold Settings

To configure threshold settings:

Step 1 From the GO menu, select **Configure > Threshold Settings**. The default values are shown for each parameter.

Step 2 Enter the new value in the New Value column.

Step 3 Click **OK**.

Top 10 Workspace Content

Table 3-14 Top 10 Workspace Content

Contents	Description
(H) Ping Response Time	Displays the top devices based on their current ping response time.
(H) Ping Packet Loss	Displays the top devices based on their current ping packet loss.
(H) CPU Utilization	Displays the top devices based on their current CPU utilization.
(H) Memory Utilization	Displays the top devices based on their current memory utilization.
(H) Disk Utilization	Displays the top devices based on their current disk utilization.
(H) Disk Free Space	Displays the top devices based on their current disk free space.
(H) Interface Utilization	Displays the top devices based on their current interface utilization.
(H) Interface Traffic	Displays the top devices based on their current interface traffic.

Table 3-14 Top 10 Workspace Content (continued)

Contents	Description
(H) Custom WMI/SNMP	Displays the top devices based on their current custom WMI/SNMP.
(H) Ping Availability	Displays the top devices based on their current ping availability.

About the Workspace Content Menu

Each workspace content type has a menu on the right side of its title bar. From the workspace content menu, you can access help, go to the configuration dialog, or close the content. Closing the content removes it from a workspace view. Keep in mind that after you remove workspace content from a workspace, any customization you have made to the workspace content is lost.

Configuring Workspace Content

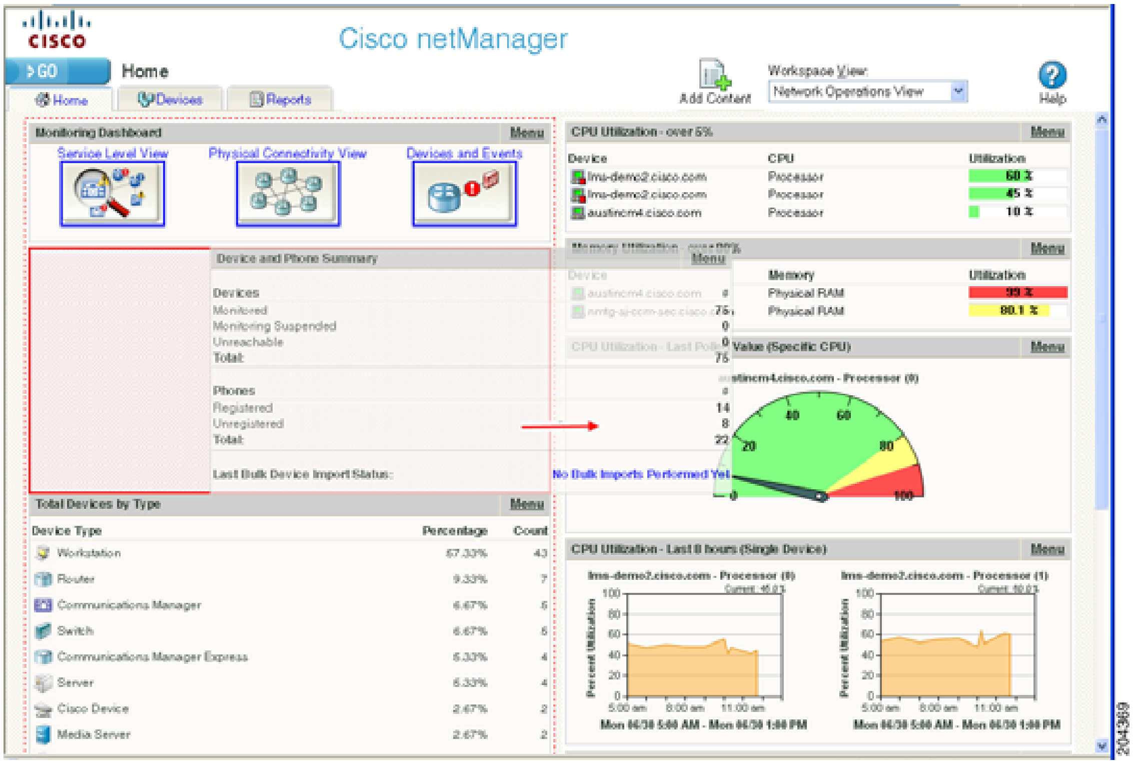
Workspace content is designed for customization to fit your own specific display needs. From a workspace content’s menu, select **Configure** to bring up its Configuration dialog. On the Configuration dialog, you’ll have the chance to do a number of things, including:

- Changing the content title
- Selecting a device or device group for the content
- Changing the height and width of the content
- Changing the width of certain content columns

Moving Workspace Content Within a Workspace

Cisco netManager supports click-and-drag within the web interface, see Table 3-14. You can move workspace content types from one column of a workspace view to another by selecting it and dragging it to another area of the workspace view. These location changes are saved: workspace content will appear in the same location to which you moved it after you log off from the web interface, or after you move between workspace views.

Figure 3-4 Moving Workspace Content



Workspace View: Network Operations View

CPU Utilization - over 5%

Device	CPU	Utilization
lms-demo2.cisco.com	Processor	60 %
lms-demo2.cisco.com	Processor	45 %
austincm4.cisco.com	Processor	10 %

Memory Utilization - over 80%

Device	Memory	Utilization
austincm4.cisco.com	Physical RAM	99 %
nmtg-sj-ccm-sec.cisco.c	Physical RAM	80.1 %

Value (Specific CPU)

Device and Phone Summary

Devices	#
Monitored	75
Monitoring Suspended	0
Unreachable	0
Total:	75

Phones	#
Registered	14
Unregistered	8
Total:	22

Last Bulk Device Import Status: No Bulk Imports Performed Yet

Total Devices by Type

Device Type	Percentage	Count
Workstation	57.33%	43
Router	9.33%	7
Communications Manager	6.67%	5
Switch	6.67%	5
Communications Manager Express	5.33%	4
Server	5.33%	4
Cisco Device	2.67%	2
Media Server	2.67%	2

CPU Utilization - Last 8 hours (Single Device)

.

CHAPTER 4

Using Topology Views

There are two types of topology views available in Cisco netManager: the Service Level View and the Physical Connectivity View.

Note The Service Level View is available only if you have purchased a license that monitors Unified Communication devices.

Using the Service Level View

Note The Service Level View is available only if you have purchased a license that monitors Unified Communication devices.

Cisco netManager's Service Level View displays a logical topology view of your Cisco Unified Communications network. You can access the Service Level View from your Home Page View or from **GO** > **Views** > **Service Level**.

The Service Level View shows all the Cisco Unified Communications Manager clusters: all instances of Cisco Unified Communications Manager Express, associated gateways and application servers. The Service Level View is designed so that you can set it up and leave it running, providing an ongoing monitoring tool that signals you when something needs attention.

Note When changing a Cisco Unified Communications application's registration from one Cisco Unified Communications Manager cluster to another, you must remove the registration of the application to the old Cisco Unified Communications Manager cluster in both the application and the old Cisco Unified Communications Manager cluster. If you do not do this, registration of the application with the old Cisco Unified Communications Manager cluster will continue to appear in the Down state in the Service Level View.

You can use the Service Level View to:

- Display a logical topology view of your Unified Communications deployment. See Starting the Service Level View, page 4-2.

- View recent events releated to the IP telephony devices associated with Cisco Unified Communications Manager clusters. This allows you to see a visual representation of your Unified Communications deployment while, at the same time, actively monitoring all devices in your network.
- Run other Cisco netManager tools. For more information, see Launching Network Tools, page 4-13.
- Launch administration pages for devices. For more information, see Launching Administration Pages for Devices, page 4-13.

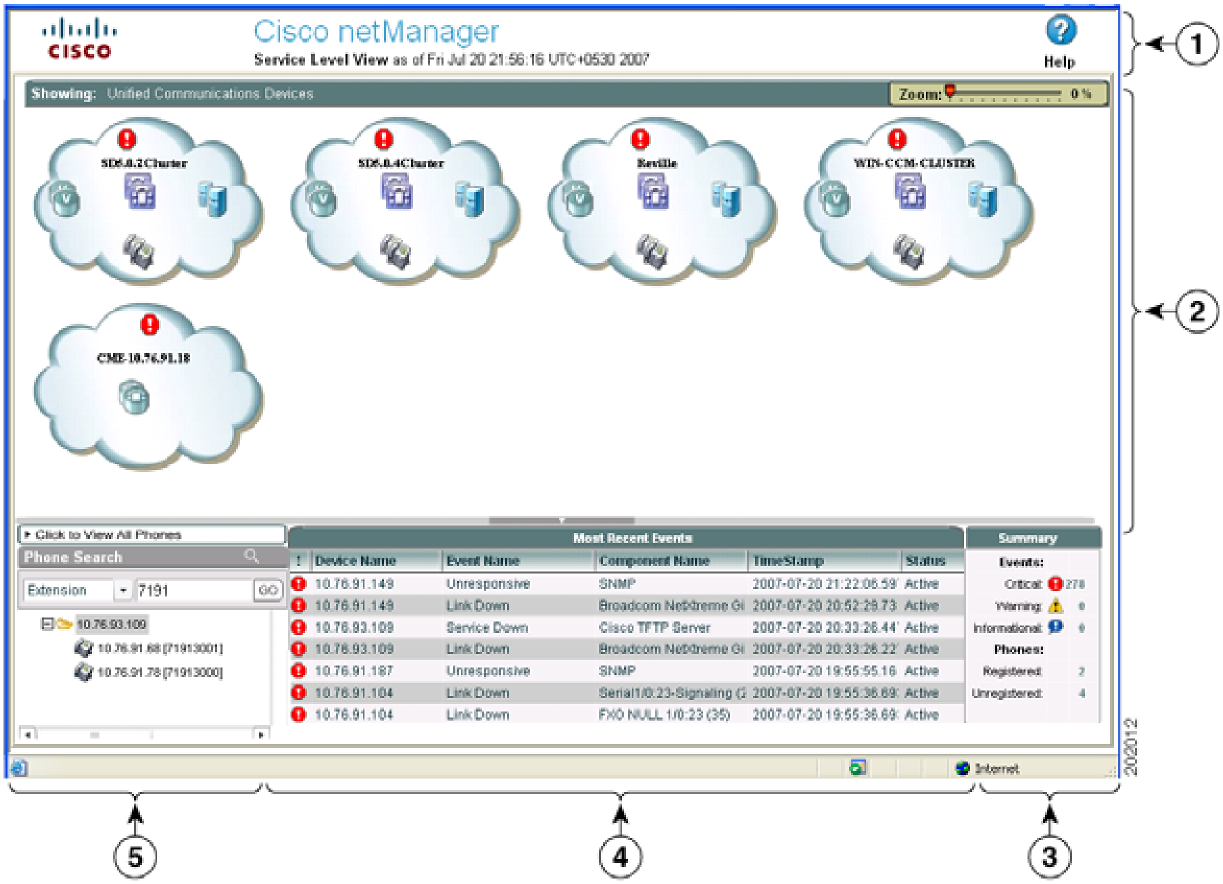
Starting the Service Level View

To start the Service Level View, select **GO** > **Views** > **Service Level View**.

Understanding the Layout of the Service Level View

Figure 4-1 shows an example of the Service Level View.

Figure 4-1 Service Level View



Most Recent Events

!	Device Name	Event Name	Component Name	TimeStamp	Status
●	10.76.91.149	Unresponsive	SNMP	2007-07-20 21:22:06.59'	Active
●	10.76.91.149	Link Down	Broadcom NetXtreme Gi	2007-07-20 20:52:29.73	Active
●	10.76.93.109	Service Down	Cisco TFTP Server	2007-07-20 20:33:26.44'	Active
●	10.76.93.109	Link Down	Broadcom NetXtreme Gi	2007-07-20 20:33:26.22'	Active
●	10.76.91.187	Unresponsive	SNMP	2007-07-20 19:55:55.16	Active
●	10.76.91.104	Link Down	Serial1/0:23-Signaling (:	2007-07-20 19:55:36.69:	Active
●	10.76.91.104	Link Down	FXO NULL 1/0:23 (35)	2007-07-20 19:55:36.69:	Active

Summary

Events:	
Critical: ●	278
Warning: ⚠	6
Informational: ●	6
Phones:	
Registered:	2
Unregistered:	4

1	**Launch Information and View Status Bar Area**—The launch information area shows the time on the server when the Service Level View was started. The view status bar lists the selected view, which is shown in the map display pane.	4	**Most Recent Events Pane—**This displays real-time active monitoring and displays the top 7 critical events sorted by severity and the time the event occurred (including those devices not represented in the map). You can sort these events by clicking the column name.
2	**Map Display Pane**—The map display pane shows a map-based view. For details on working with the map display pane, see Map Display Pane, page 4-4.	5	**Phones Pane**—The phones pane allows you to locate a phone or view a phone's reports.
3	**Summary Pane**—Displays the total number of critical, warning and informational events. It also displays the number of registered and unregistered phones.		

Phones Pane

In the phones pane, you can search for a specific phone endpoint and view the phones report. For more information, see the following topics:

- Using the Search Tool to Locate a Phone, page 4-3
- Launching a Phone Report from the Service Level View, page 4-3

Using the Search Tool to Locate a Phone

When you click a phone from the phone endpoint search results, the map display pane displays a drilled-down view, with the phone highlighted. The phone will have a logical link to the Cisco Unified Communications Manager to which it is registered.

Step 1 In the search field located in the phones pane, select whether you want to search by extension number, IP address, or MAC address.

Step 2 Enter the appropriate number for the phone.

Step 3 Click **Go**.

Launching a Phone Report from the Service Level View

Step 1 Do one of the following:

- Click **Click to View All Phones** in the phones pane. The phones report for all phones opens in another window.
- Right-click a phone or a Cisco Unified Communications Manager icon in the map display pane, then select **Associated Phones**. The phones report for the selected phone opens in another window.

Map Display Pane

The map display pane shows the registration status of IP telephony devices. This information is displayed in a map-based view. You can drill down to devices in the display pane by clicking the cluster cloud. To get back to the cluster cloud view, click the Unified Communications Devices link (located just at the bottom of the View Status Bar Area).

Drilling down on these clouds shows the individual devices with relevant information. This gives you a quick snapshot of the overall health of your Unified Communications network.You can easily locate devices and links that may cause problems and view the underlying infrastructure of your Unified Communications network.You can view link or port status and device information by moving your cursor over any link or device icon. For more information on device icons and links, see Topology Views Legend, page 4-7. In general, the colors of the icons represent the following:

- Green—Devices that are managed by Cisco netManager.
- Gray—Devices that are not managed by Cisco netManager.
- Red—Devices that are down.

Note If a device icon is not connected to anything, it means that Cisco netManager is unable to get its connectivity details because CDP protocols are not enabled on the device.

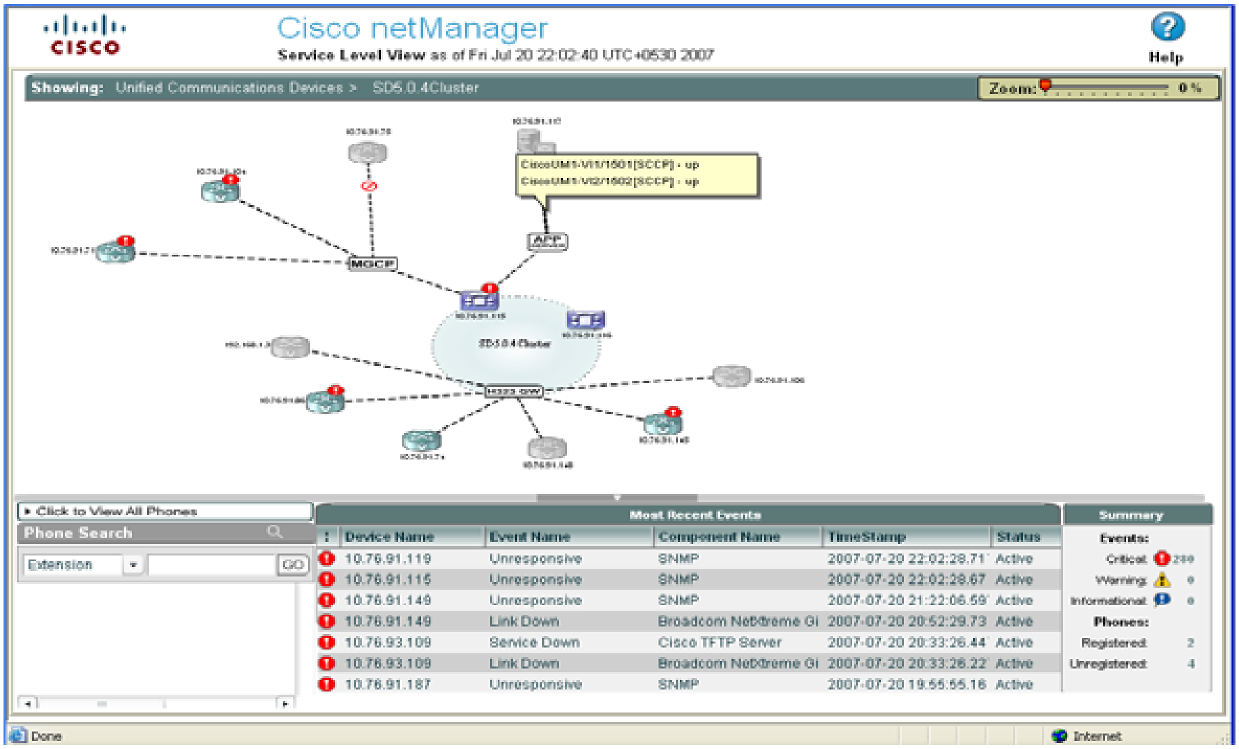
For example, in Figure 4-2, the following Service Level View information is displayed:

- The large circle represents the logical grouping of Cisco Unified Communications Managers in this cluster.
- The H323 icon shows that the voice gateways are registered to the cluster using H323 protocol.
- Three of the voice gateways are not monitored by Cisco netManager. Two of the managed voice gateways and the Cisco Unified Communications Manager Express have issued critical events.
- The MGCP icon shows that the voice gateway connected to the Cisco Unified Communications Manager is using MGCP protocol. Both devices have issued critical events.
- The APP Server icon shows that other IP telephony applications are connected to a Cisco Unified Communications Manager. In this example, a Cisco Unity device (voicemail server) is connected to the Cisco Unified Communications Manager.
- A tooltip displays useful information about a device or link. A tooltip appears after you move your cursor over a link or device. In this example, it displays the Cisco Unity ports’ registration status with the Cisco Unified Communications Manager.
- Gray device icons represent devices that are not managed by Cisco netManager. If you want to monitor all IP telephony devices within the cluster, you can add the device. For more information on adding devices, see Adding a New Device, page 2-4.
- Blue or green device icons represent devices that are managed by Cisco netManager.
- Red icons represent devices that are down.
- Devices that have alerts will have critical (red), warning (yellow), or informational (blue) icons in the upper-right corner of the device icon. See the Summary Pane to view actual representations of icons.

Note If a device is not part of a cluster, it will not be shown.

Note To enlarge or reduce the size of the map display, use the size slider at the top of the pane. The size slider can be used in either the Service Level View or Physical Connectivity View.

Figure 4-2 *Map Display of Service Level View*


Cisco netManager
Service Level View as of Fri Jul 20 22:02:40 UTC+0530 2007
Help
Showing: Unified Communications Devices > SD5.0.4Cluster
Zoom: 0 %
CiscoUM1-VI1/1501[SCCP] - up
CiscoUM1-VI2/1502[SCCP] - up
APP
MGCP
SD5.0.4Cluster
H323 GW
Click to View All Phones
Phone Search
Extension
GO
Most Recent Events
Summary
Done
Internet
202011

!	Device Name	Event Name	Component Name	TimeStamp	Status
!	10.76.91.119	Unresponsive	SNMP	2007-07-20 22:02:28.71	Active
!	10.76.91.115	Unresponsive	SNMP	2007-07-20 22:02:28.67	Active
!	10.76.91.149	Unresponsive	SNMP	2007-07-20 21:22:06.59	Active
!	10.76.91.149	Link Down	Broadcom NetXtreme Gi	2007-07-20 20:52:29.73	Active
!	10.76.93.109	Service Down	Cisco TFTP Server	2007-07-20 20:33:26.44	Active
!	10.76.93.109	Link Down	Broadcom NetXtreme Gi	2007-07-20 20:33:26.22	Active
!	10.76.91.187	Unresponsive	SNMP	2007-07-20 19:55:55.16	Active

Events:	
Critical:	299
Warning:	0
Informational:	0
Phones:	
Registered:	2
Unregistered:	4

Using the Physical Connectivity View

The Physical Connectivity View gives you a visual representation of all physical devices and connections in your network. This view gives a quick snapshot of your entire network, including its overall health. From the Physical Connectivity View, you can easily see which devices and connections are down.

Note

- Once a device is added, it may take some time for it to be discovered and appear in the Physical Connectivity View.
- To enable you to view lightweight access points, CDP must be enabled and all connected switches added to the Cisco netManager database.

You can view link or port status and device information by moving your cursor over any link or device icon. For more information on device icons and links, see Topology Views Legend, page 4-7. In general, the color of the icons represent the following:

- Green—Devices that are managed by Cisco netManager.
- Gray—Devices that are not managed by Cisco netManager.

- Red—Devices that are down.
- Devices that have alerts will have critical (red), warning (yellow), or informational (blue) icons in the upper-right corner of the device icon. See the Summary Pane to view actual representations of icons.

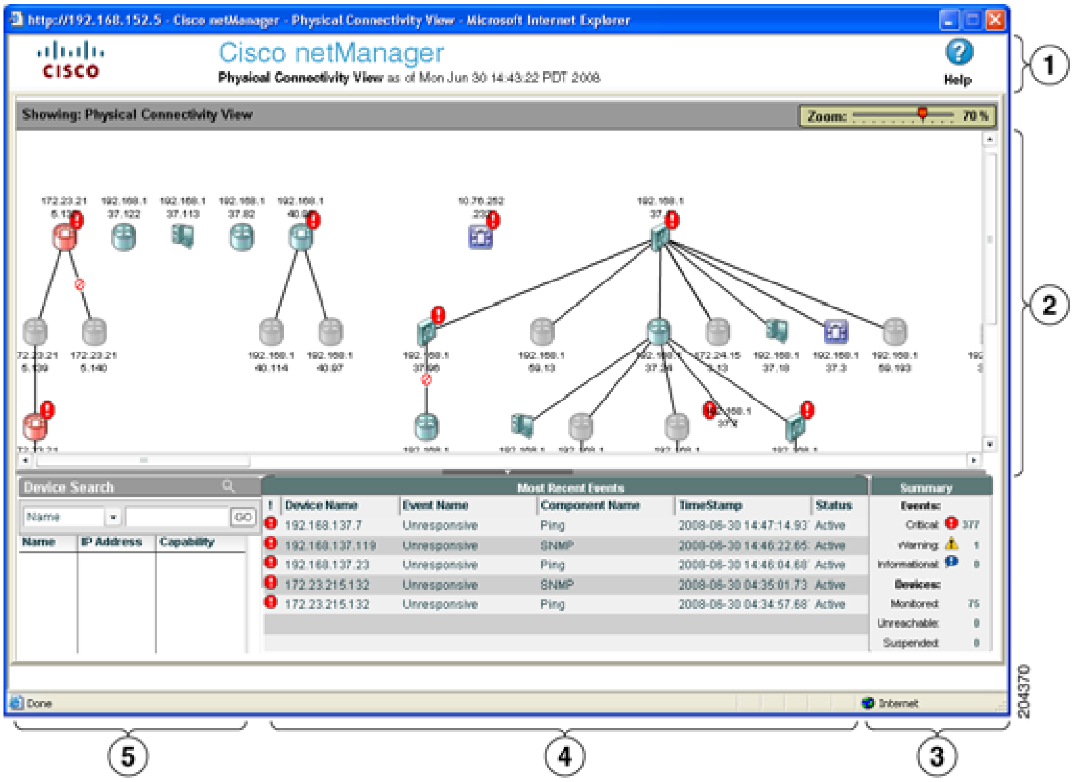
Note If a device icon is not connected to anything, it means that Cisco netManager is unable to get its connectivity details because CDP protocols are not enabled on the device.

From within the Physical Connectivity View, you can also launch several Cisco netManager tools, external applications, and device administration pages. To access these tools and applications, right-click an object in the view; the available options are displayed in a menu box. For more information, see Launching Network Tools, page 4-13.

Understanding the Layout of the Physical Connectivity View

Figure 4-3 shows an example of the Physical Connectivity View.

Figure 4-3 Physical Connectivity View


http://192.168.152.5 - Cisco netManager - Physical Connectivity View - Microsoft Internet Explorer
CISCO
Cisco netManager
Physical Connectivity View as of Mon Jun 30 14:43:22 PDT 2008
Help
Showing: Physical Connectivity View
Zoom: 70 %
Device Search
Name
GO
Name
IP Address
Capability
Most Recent Events
Summary
Done
Internet
204370
1
2
3
4
5

!	Device Name	Event Name	Component Name	TimeStamp	Status
●	192.168.137.7	Unresponsive	Ping	2008-06-30 14:47:14.93	Active
●	192.168.137.119	Unresponsive	SNMP	2008-06-30 14:46:22.65	Active
●	192.168.137.23	Unresponsive	Ping	2008-06-30 14:46:04.60	Active
●	172.23.215.132	Unresponsive	SNMP	2008-06-30 04:35:01.73	Active
●	172.23.215.132	Unresponsive	Ping	2008-06-30 04:34:57.68	Active

Summary	
Events:	
Critical ●	377
Warning ⚠	1
Informational ●	0
Devices:	
Monitored:	75
Unreachable:	0
Suspended:	0

1	**Launch Information and View Status Bar Area**—The launch information area shows the time on the server when the Physical Connectivity View was started. The view status bar lists the selected view, which is shown in the map display pane.	4	**Most Recent Events Pane—**This displays real-time active monitoring and displays the top 7 critical events sorted by severity and time the event occurred (including those devices not represented in the map). You can sort these events by clicking the column name.
2	**Map Display Pane**—The map display pane shows a map-based view. For details on working with the map display pane, see Map Display Pane, page 4-4.	5	**Device Search**—The devices can be searched on the map based on IP Address or Display Name.The results of search are shown in a table (with columns for IP address, display name, and capability) and are highlighted on the map. When a row in the table is clicked, the map is zoomed to 100% and the scrollbars positioned to show the corresponding device in the visible area of the map. The Display Name search string can be any string. The IP Address has to be in the form of four octets: [0-255].[0-255].[0-255].[0-255]. An asterisk ('*') can be used in place of any of the octets like a wildcard.
3	**Summary Pane**—Displays the total number of critical, warning and informational events.		

Starting the Physical Connectivity View

To start the Physical Connectivity View, do one of the following:

- Select **GO** > **Views** > **Physical Connectivity View**.
- From Home page, select the Physical Connectivity View icon.

Displaying IP Address or Display Name

To have devices display on the Physical Connectivity View by IP address, display name, or both, do the following:

Step 1 Select **GO** > **Configure** > **Physical Connectivity View Settings**.

Step 2 Check **IP address**, **Display Name**, or both.

Topology Views Legend

Table 4-1 and Table 4-2 describe the icons and the link status that can appear in both topology views.

Table 4-1 Device Icons for Topology Views

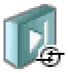
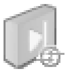
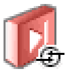
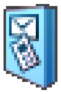
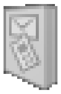
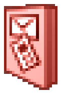
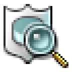
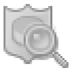
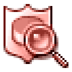
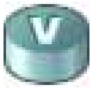
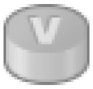
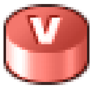
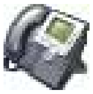
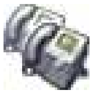
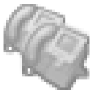
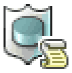
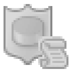
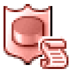
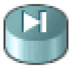
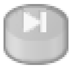
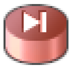
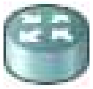
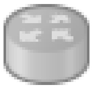
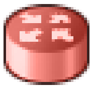
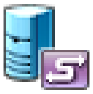
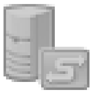
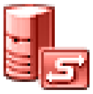
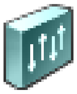
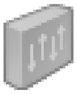
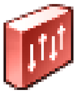
Icon (Monitored)	Icon (Not Monitored)	Icon (Event)	Description
			Cisco ASA.
			Cisco Contact Center Express.
			Cisco IDS.
			Gatekeeper.
	—	—	IP phone.
		—	Group of IP phones.
			Cisco IPS.
			Cisco PIX.
			Router.
			SIP endpoint.
			Switch.

Table 4-1 Device Icons for Topology Views (continued)

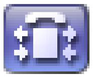
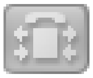
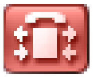
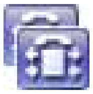
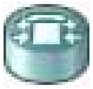
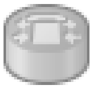
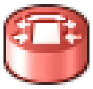
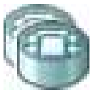
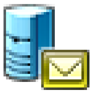
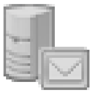
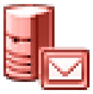
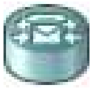
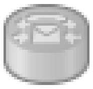
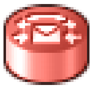
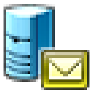
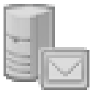
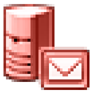
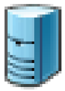
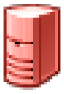
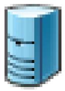
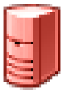
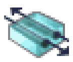
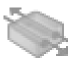
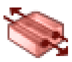
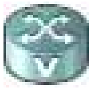
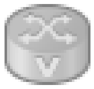
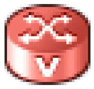
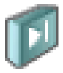
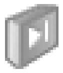
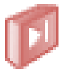
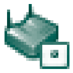
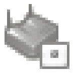
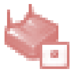
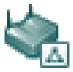
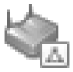
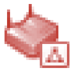
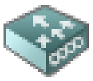
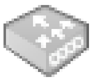
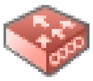
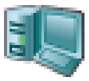
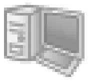
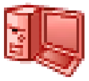
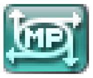
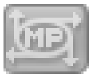
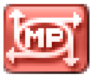
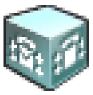
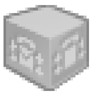
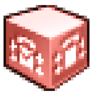
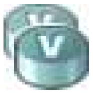
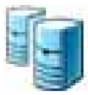
Icon (Monitored)	Icon (Not Monitored)	Icon (Event)	Description
			Cisco Unified Communications Manager.
	—	—	Cisco Unified Communications Manager Group.
			Cisco Unified Communications Manager Express.
	—	—	Cisco Unified Communications Manager Express Group.
			Cisco Unity.
			Cisco Unity Express.
			Cisco Unity Connection.
	—		Cisco Unified Presence Server.
	—		Voice application server.
			Cisco Virtual Private Network (VPN).

Table 4-1 Device Icons for Topology Views (continued)

Icon (Monitored)	Icon (Not Monitored)	Icon (Event)	Description
			Voice Gateway.
			Cisco Firewall Service Module (FWSM).
			Autonomous Access Point.
			Lightweight Access Point (LWAP).
			Wireless LAN Controller.
			Workstation.
			Cisco Unified MeetingPlace Express.
			Rich Media appliance.
	—	—	Voice router group. This icon appears in the first-level cloud view and represents the capability of the cluster in the cloud.
	—	—	Group of IP phone applications. This icon appears in the first-level cloud view and represents the capability of the cluster in the cloud.

Note To enlarge or reduce the size of the map display, use the size slider at the top of the pane. The size slider can be used in either the Service Level View or the Physical Connectivity view.

Table 4-2 Link Type Description for Topology Views

Link	Description
——⊘——	Physically connected, but the connection is down.
——⚠——	Physically connected, but one of the multiple connections is down.
————	Physically connected, and the connection is up.
- - - - -⊘- - - - -	Logically connected, but registration status is down.
- - - - -⚠- - - - -	Logically connected, but registration status is down.
- - - - - - - - - - - -	Logically connected and registration status is up.

Launching Cisco netManager Tools

You can access several Cisco netManager tools as well as external applications through both topology views.

Note You will have access to these tools only if you have proper authorization.

You can do the following:

- View and acknowledge event information for a device (see Viewing Events Information, page 4-12 and Acknowledging All Device Events, page 4-12).
- View events and event history for a device (see Viewing Device Information, page 4-12).
- View device information (see Viewing Device Information, page 4-12).
- View associated phones for a Cisco Unified Communications Manager (see Viewing Phones Report, page 4-12).

- Launch administration pages for devices (see Launching Administration Pages for Devices, page 4-13).
- Launch external applications (see Launching Network Tools, page 4-13).

Viewing Events Information

Step 1 Right-click the device for which you want to view event information.

Step 2 From the menu, select **Events**. The Event Report opens in a separate window. For more information, see Events, page 11-16.

Acknowledging All Device Events

Step 1 Right-click the device for which you want to view event information.

Step 2 From the menu, select **Acknowledging All Device Events.** A confirmation window appears.

Step 3 Click OK to acknowledge all events for the selected device.

Viewing Device Information

Step 1 Right-click the device for which you want to view information.

Step 2 From the menu, select **Detailed View**.

Step 3 The Device Status Workspace window appears. For a description of the Device Status Workspace, see Device Status Workspace, page 3-2.

Viewing Phones Report

You can view an associated phones report. If you are viewing an associated phones report for a switch, the report displays the phones that are connected to the switch. If you are viewing an associated phones report for a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, the report displays all the phones connected to the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, registered or unregistered.

Step 1 In the map display pane, right-click the phone, Cisco Unified Communications Manager, or Cisco Unified Communications Manager Express for which you want to view associated phones.

Step 2 From the menu, select **Associated Phones**.

The Associated Phones report for the selected device appears.

Launching Administration Pages for Devices

Some devices will allow you to launch their administration pages. The availability of these pages depends on the device type. For example, Cisco Unified Communications Manager and Cisco Unity devices provide access to their administration pages.

Step 1 Right-click the device whose administration page you want to open.

Step 2 From the menu, select the administration page link.

The following list shows the possible options (depending on the device):

- Cisco Unified Communications Manager Administration
- Cisco Unified Communications Manager Express Administration
- Cisco Unified Communications Manager Serviceability
- Cisco Unity Administration
- Cisco Unity Connection Administration
- Cisco Unity Express Administration

The administration page opens.

Connecting to the Device Using Web Launch

Step 1 Right-click the device you want to connect to.

Step 2 From the menu, select **Web Launch**.

Step 3 Enter the username and password for the device.

Launching Network Tools

Each view provides you with launching points for network tools that help you check on the connectivity of network devices. You can launch several external applications:

- Ping Tool, page 4-14
- DNS Lookup Tool, page 4-14
- Trace Route Tool, page 4-14
- Telnet Tool, page 4-15
- MAC Address Tool, page 4-15

Note You can also access these tools from the context-sensitive menu available on the Devices Tab or from the **GO** menu. For more information, see the Context-Sensitive Menu, page 2-3 or Using the GO Menu, page 1-4.

Using the Ping Tool

This tool sends out an Internet Control Message Protocol (ICMP) echo request to the network device identified in the Address/Host name field. The results of this request appear on the right side of the page after the request has been made.

Step 1 Right-click the device you want to connect to.

Step 2 From the menu, select **Ping**. The following fields appear:

Address/Host name—The target of the ping echo request. Enter the hostname or IP address of the device you want to check.

Timeout—Enter the amount of time (in milliseconds) for the tool to wait for a response from the device. The Ping fails if this time limit is exceeded.

Count—Enter the number of data packets sent by the Ping tool.

Packet size—Enter the size (in bytes) of the packets you want the Ping tool to send. 32 bytes is the default.

Results:

- **Result**—Success or Failure.
- **RTT**—Round trip time; the amount of time it takes for the ping request to be returned from the remote device.
- **Address**—The IP address of the device

Using the DNS Lookup Tool

Lookup is a debugging tool that lets you query your Internet domain name system (DNS) server for information about a domain and its registered hosts. Lookup can show you what happens when an application on your network uses your DNS server to find the address of a remote host.

Step 1 Right-click the device you want to connect to.

Step 2 From the menu, select **Lookup**. The following fields appear:

Address/Host name—Enter the hostname or IP address of the device you want to trace the route to.

Lookup Type—Select the lookup type from the drop-down list.

A—Look up the host's Internet address from the hostname.

PTR—Look up the hostname from the Internet address.

Using the Trace Route Tool

This tool sends out echo requests to a specific device, then traces the path it takes to get to that IP address or hostname. This is useful in finding out where on your network an interruption occurs.

Step 1 Right-click the device you want to connect to.

Step 2 From the menu, select **TraceRoute**. The following fields appear:

Address/Host name—Enter the host name or IP address of the device you want to trace the route to.

Timeout—Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The trace route fails if this time limit is exceeded.

Max hops—Enter the maximum number of hops you want to limit the route to. Usually, 32 hops should be enough to find any device on the Internet.

Result—Success or Failure. This is the general result of each hop in the trace route process.

RTT #1/#2/#3—The tool sends out three ping requests to each hop in the route to the device. These columns show the round-trip time for each of the requests.

Address—The IP address of each device encountered on the path.

Host name—The host name of each device encountered on the path.

Using the Telnet Tool

Step 1 Right-click the device you want to connect to.

Step 2 From the menu, select **Telnet**. This launches a Telnet session for the device.

Using the MAC Address Tool

This tool enables you to discover what MAC addresses are present on your network and gives you the opportunity to obtain physical connectivity information for devices on your network. This tool helps you solve IP address conflicts within your network by providing you with specific switch information.

Step 1 Enter or select the appropriate information into the following fields:

- **Local subnet**—Enter the subnet you would like to find MAC addresses for.
- **Get connectivity information from using SNMP**—If you would like switch-specific connectivity information for a device in the network, select this option.
- **Switch IP address**—Enter the switch IP address.
- **SNMP credential**—Select the SNMP credential that you use to poll this device.
- **Timeout**—Enter the amount of time (in milliseconds) for the tool to wait on a response from the switch. The MAC address discovery fails if this time limit is exceeded.
- **Retry**—Enter the maximum number of retries when polling the switch using SNMP.
- **Show results in new window**—Select this option to have the results displayed in a new window.
- **Show results in formatted mode**—Select this option to have the results displayed in a table format.

Step 2 Click **Discover** to run the test.

The results of the test are displayed at the bottom of the page:

Result—Success or Failure. There are two different results for the MAC address discovery and the physical connectivity information discovery.

MAC address discovery

- **IP address**—The IP addresses in your network.
- **MAC address**—The MAC addresses in your network.
- **DNS name**—The DNS names that coincide with your network's IP addresses.

SNMP connectivity information discovery

- **IP address**—The IP addresses of your network.
- **MAC address**—The MAC addresses in your network.
- **DNS name**—The DNS names that coincide with your network's IP addresses.
- **Port #**—The port numbers of the switch ports that are connected to the devices that own the listed MAC addresses.
- **Interface Index**—The unique value assigned to each interface. This number typically corresponds with the interface port number.
- **Interface description**—Listed as a letter and a numeral; for example, "Ethernet 5" or "B4." The interface description allows you to identify the physical connector on the switch.

CHAPTER 5

Polling

Polling is the active watching, or monitoring, of your network by Cisco netManager. This is done in a variety of ways, depending on the service monitors you have configured on your devices. The default polling is done through ICMP. The default polling interval for Cisco netManager is 60 seconds for active monitors. The default polling interval for performance monitors is 180 seconds. The polling interval for performance monitors can be configured.

Only a subset of the device data—data related to device or service status and statistical data—is polled each time. Static data such as version information, description, and so on is collected when the device is discovered. If there is a need to refresh this data, the device will need to be rediscovered. See Rediscovering Devices, page 2-14 for more information on how to rediscover devices.

A small amount of data is sent from the Cisco netManager computer across the network to the device it is watching. If the device is up, it echoes the data back to the Cisco netManager computer. Cisco netManager considers a device down when it does not send the data back.

Changing How You Poll Devices

After a device is added to the database, Cisco netManager begins watching that device using ICMP . Cisco netManager sends a message to the device, then waits for the echo reply. If the reply is not returned, Cisco netManager considers it an unresponsive device and changes the status color of the device.

By default, Cisco netManager uses the IP address of the device to send this message. You can change this to use the hostname or the Windows name of the computer, and you can change the means Cisco netManager uses to poll the devices.

Step 1 From the Devices tab, right-click the device and select **Properties**.

Step 2 Click the **General** icon.

Step 3 Select the type of poll you want to check the device with in the **Polling type** list box.

Step 4 Select an IP address or hostname from the Poll using list box.

Step 5 If you selected hostname in the Poll using box, complete the hostname box.

Step 6 Click **OK** to save changes.

Using Maintenance Mode

This feature lets you place devices in Maintenance mode, where they will not be polled by the engine.

Any device placed in maintenance mode is not polled, and actions are not fired for it, but it remains in the device list and historical data is preserved. By default, maintenance mode is represented by an orange color in both the device list view and the map view.

The mode can be set in two ways:

- **Force this device into maintenance mode now**—Set this option manually by selecting **Device Properties > Polling**.
- **Scheduled maintenance times—**Schedule maintenance times for the device.
  - Click **Add** to schedule a new maintenance time for the device.
  - Select an existing entry, then click **Edit** to change a scheduled time.
  - Select an existing entry, then click **Remove** to delete a scheduled time from the list.

Setting the Polling Interval

The default polling interval is 60 seconds. You can change this on a per-device basis.

Step 1 From the Devices tab, right-click the device and select **Properties**.

Step 2 Click the Polling icon.

Step 3 Change the interval in the Poll Interval box.

Step 4 Click **OK** to save changes.

Stopping and Starting Polling

To stop or start polling on all devices by enabling or disabling the polling engine:

Step 1 From the main menu, click **Configure > Program Options.**

Step 2 Click the **General** icon.

Step 3 Select **Enable polling engine** to enable polling. Clear the selection to disable polling.

Step 4 Click **OK** to save changes.

In the bottom right corner of the Cisco netManager console, the Polling icon shows if the engine is active or not.

Stopping and Starting Polling On a Monitor

To stop and start polling on a per-monitor basis:

Step 1 From the Devices tab, right-click the device and select **Properties**.

Step 2 Click the **Active Monitor** icon.

Step 3 Select the active monitor you want to change the polling on.

Step 4 Click **Edit** to view the Monitor Properties for that monitor.

Step 5 Click the **Polling** icon.

Step 6 Select **Enable polling for this Active Monitor** to enable polling, or clear the option to disable it.

Step 7 Click **OK** to save changes.

Dependencies Overview

By default, Cisco netManager polls all devices and active monitors in your device list, unless you manually disable polling for the system as a whole, or at the device and monitor level. The dependency feature gives you the ability to avoid turning off polling to devices, and instead makes polling dependent on the status of another device's active monitor(s) in your database.

Setting dependencies on one device's active monitors will place another device up or down depending on the type of dependency you configure.

There are two types of dependencies:

- **Up Dependency** can be thought of as describing that something is “behind” something else. The dependent device will only be polled if the device "in front" of it is up.
- **Down Dependency** can be thought of as describing that something is “in front of” something else. The dependent devices in front will not be polled unless the device further down the line is down.

Example

If you have devices behind a router, up dependent on the router's ping active monitor, those devices will not be polled unless that router's ping attempts are successful. Should the router's ping active monitor fail, the devices behind the router will be placed in the unknown state. Without the dependency, the devices behind the router would fire off actions when they become unreachable due to the router's failed ping attempts. With the dependency, only actions on the router will fire.

Setting Dependencies

To set dependencies, double-click a device from the Devices tab and select Device **Properties> Polling**. Click either **Up Dependency...** or **Down Dependency...** to bring up the Device Dependencies dialog and configure the up or down dependency.

- Using the Map View

  In My Network view, go to **View > Map View**. Right-click a selected device and select **Set Dependencies** and either **Set Up Dependency on** or **Set Down Dependency on**. The cursor changes to the Set Dependency arrow. click any device in the current group to set the dependency. Selected **Display > Polling Dependency Arrows** to view the dependency between the two devices.

In the Map View, you are not able to set dependencies across groups. However, you can make shortcuts to the devices you want to set dependencies on in a group, and set the dependencies there.

Using the Device Dependencies Dialog

The Device Dependencies dialog is the same for both up and down dependencies with the exception that one sets up dependencies and the other sets down dependencies. Up dependencies are signified with an upward green arrow icon, while down dependencies is signified with a downward red arrow.

- Check the first box on the dialog to either poll only if Any one or Every one of the active monitors selected are up or down on device, depending on the type of dependency you are setting.
- To select a device for the dependency, click the browse **(...)** button.
- Choose either **All active monitors** or **Specific active monitors** and check the active monitors you want to associate with the dependency.

The statement at the bottom of the dialog is automatically generated for you to assist you in understanding the type of dependency you are creating.

An example statement would read:

"ATL145 is dependent on QATEST-WIN2K's FTP and HTP and Ping active monitors being up. (ATL145 is "behind" QATEST-WIN2K.)"

Viewing Dependencies

After you have set up your dependencies, you can view dependency lines in the Map view, as long as the devices appear in the same group. If the devices are not in the same group, you will have to refer to the Polling section of Device Properties to view the dependencies.

Devices have an up dependency on the router, and the router has a down dependency on the hub. If the router's active monitors were to fail, the hub would be polled, and the devices behind the router would not be polled. When the router's active monitors are successful, the hub is not polled, but the devices behind the router are.

IPX Support

To poll IPX devices, Microsoft NWLink IPX/SPX Compatible Transfer Protocol must be installed and running on the Cisco netManager console (the system on which you installed Cisco netManager).

To add the IPX protocol:

Step 1 Open the Network applet in the Windows Control Panel.

Step 2 If you are using Windows NT, in the Select Network Protocol dialog box, select Microsoft, then select the IPX/SPX-compatible protocol and follow the online instructions.

or

If you are using Microsoft Windows 2000 or XP, in the Select Network Component dialog box, select Microsoft, then select the IPX/SPX-compatible component and follow the online instructions.

CHAPTER 6

Using Actions

When a device or monitor state change occurs, Cisco netManager can perform an action to try to correct the problem, notify someone of the state change, or launch an external application.

For example, you can set up an action that sends you an e-mail alert when your web server device is down.

You can configure actions on a single device or monitor, or define an Action Policy to use across multiple devices or monitors.

Cisco netManager provides the following action types:

- **Beeper Action**—Activate a beeper.
- **Pager Action**—Send a message to a pager.
- **Program Action**—Run another program (executable) to take some action.
- **Email Action**—Send an SMTP mail message.
- **Winpop Action**—Display a message in a popup window on a Windows NT system.
- **SMS Action**—Send a Short Message Service (SMS) notification to a pager or cell phone.
- **Service Restart Action**—Stop or restart a Windows NT system.
- **Syslog Action**—Send a message to a host that is running a Syslog server.
- **Text to Speech Action**—Send a text-to-speech notification to a speaker.
- **Sound Action**—Sound an alarm by playing a sound file on the Cisco netManager console.
- **Active Script Action**—Allows you to write either VBScript or JScript code to perform a check on a device. If the script returns an error code, the monitor is considered down. Be aware that Cisco netManager does not support the scripts that you create, only the ability to use them in the Script Action.
- **Web Alarm**—Sound an alarm by playing a sound file on the Cisco netManager web interface.

About Action Strategies

When configuring actions for your devices and monitors, there are a few things you should take into consideration:

- Large lists of devices have the potential of sending out very large numbers of external notifications (e-mail, SMS, beeper, and so on).

  Imagine the number of messages sent if external notifications are placed on a router and every device and monitor that uses that router for their connection to the Internet. If the router goes down, it will appear as if all of the devices are down, and messages will be sent for each of them. Consider using dependencies and limiting the external notifications to the router and the most important of the devices in the group.
- Do not rely on sound actions when there is not someone around to hear the notification.

  Sound notifications are safe to use in almost any situation, but is not the best choice for items that need to be monitored overnight.
- If the device states do not fit what you need, change them or add new ones.

  You may want to add device states for longer periods of downtime. Consider creating a **Down at least 60 mins** state and sending an escalated message to show that the device is still down after an hour.
- Action Policies are easier to manage than lists of actions built on a device. For more information, see About Action Policies, page 6-21.

  Whenever possible, it is a good idea to use action policies over actions configured for a single device. That way, you can reuse the work you put into the list, and can keep better watch over the actions that are being fired.
- Visual notifications are usually enough for most of the devices on your network.

  Unless a device is vital to the operations of the business or office, the state change color and shape should be enough to let you know what is going on with your monitored devices.
- If you want to be notified if any or all of the monitors on a device go down, assign the action to the device. If you are concerned with specific monitors on a device, assign the action to the monitor itself. Remember that if you assign the action to both the monitor and the device, both actions will fire if the monitor goes down.

About the Action Library

The Action Library shows all of the actions configured for your network. These actions can be assigned to any device or monitor, or included in an action policy. When you assign the action to a device or monitor, you specify the state change that will trigger the action.To open the Action Library, from the main menu of the Cisco netManager console, select **Configure > Action Library**.

From this dialog, you can:

- **Create a new action**—Click **New.** After the action has been created, it can be associated to one or multiple devices or monitors. You can create the following types of actions to send a message or take an action when the status of a device or monitor changes:
  - Beeper
  - Sound
  - Pager

  - Program
  - Service Restart
  - SMS
  - SMTPMail
  - Syslog
  - Text to Speech
  - WinPopup
  - Web Alarms
  - Action Script

- **Make changes to an action**—Select the action you want to modify and click **Edit**. Changes made here affect each instance of the action.
- **Copy an action**—To create a copy of an action so you can base a new action on the setup information of an existing one, select the action and click **Copy**. You can then edit the new copy as needed.
- **Remove an Action from the Action Library and devices and monitors**.—To remove an Action from both the Action Library and any device or monitor to which it is assigned, select the action, then click **Delete**. This is a global delete of the selected action; the action is removed from any action policy, device, or active monitor to which the action is associated.

If you need to remove an action from a specific action policy, device, or monitor, open the properties for the policy, device, or monitor and delete it there. This removes only the specified instance of that action; the action remains in the Action Library and on other devices to which it is assigned.

Note Be aware that when you remove an action from the Action Library, you are removing that action from all action policies, as well as all devices and monitors that the action is assigned to. In addition, all statistics relating to that action are also deleted from the database. When you first open the Action Library, if you have not yet defined an Action, you will see the default Web Alarm, which you can assign to any device or monitor.

Configuring an Action

There are two aspects of fully configuring an action. The first is to create the action itself in the Action Library dialog. The setup consists of:

- Defining the target of the action (for example, a pager or e-mail address)
- Entering the notification variables or program arguments (which specify what information to report in the action message or to pass to another program).

After the action has been created, the second step is to assign the action or action policy to a device or active monitor and to link it to a state change (action policies are already linked to a state change during the policy definition). For more information see:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16
- Creating an Action Policy, page 6-21

After the actions have been completely configured, Cisco netManager launches the action as soon as the proper state change is reached.

Action Builder Wizard

The Action Builder Wizard is used to associate an action with a state change for the current device or monitor. Use this wizard to set up an action to be executed when the specified state change occurs. New actions created through the wizard are added to the Action Library. After the action has been added to the library, it can be assigned to any device, active monitor, or action policy in your database.

- **Fire an action when the monitor enters the following state**—Select a state from the pull-down list. The assigned action launches as soon as the polling engine determines that the device or monitor has reached this state.
- **Action to Fire**—Select a configured action from the pull-down list, or click the Browse button to access the Action Library. The Action Library is used to configure these actions for use across the application.

Access the wizard in any of three ways:

- Go to **Device Properties** > **Actions**, then click **Add**.
- Go to **Device Properties** > **Active Monitors** > **Monitor Properties** > **Actions**, then click **Add**.
- On the Actions Policies dialog, click **Add**.

Creating a Beeper Action

Step 1 From the GO menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Beeper Action**.
- Select an existing Beeper Action, then click **Edit**. The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter the name of the action as it appears in the Action library.
- **Description**—Enter a short description of the action. This is displayed in the Action Library dialog along with the entry in the Name box.
- **Beeper number**—Enter the phone number to dial. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers; for example, (617) 555-5555.
- **Pause after answer**—Enter a number of seconds the modem should pause before sending the signal codes once a connection has been made.
- **End transmission**—By default, # is the correct symbol for the end transmission command. Some international systems require other or additional symbols.
- **Modem setup**—Select either Primary or one of the alternate setups. Click Port Settings to further define your selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your beeper notifications. There could also be times you want to change your settings to meet a specific service provider's requirements for a specific notification (for example, a lower baud rate). To do this, you can set do an alternate modem setup and associate this to the notification instead of using your primary setting.

Note Changing the port settings for the desired modem setup will affect *all* uses of that setting.

- **Up code**—Specifies the characters sent to the beeper to indicate that the device has come back up after being down (the default value is 0*).
- **Down Code**—Specifies the code sent to indicate the device is down (the default value is 1*).
- **On passive monitor code**—Specifies the code sent to indicate that an active monitor has been received for the device. (Default value is 2*) You can use the asterisk (*) character to separate codes from a subsequent message.
- **Recurring action code**—The percent variable for the action. The default action codes are:
  - %System.NumberofUpDevices
  - %System.NumberofDownDevices

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Port Settings

The port settings dialog box contains the following options:

- **Modem Initialization String (ATE0)**—The default string is ATE0Q0V1X4F1.
  - (E0) Command Echo Off
  - (Q0) results code
  - (V1) verbal results code (as opposed to numeric)
  - (X4) result codes for some specific phone/modem conditions (see modem manufacturer for details)
  - (F1) local echo off
- **COM Port**—Select the port to which your modem is attached.
- **Baud Rate**—Select the speed (measured in bits per second) at which the serial port will communicate with the modem.

Note Newer modems (for example, 56K versions) may be utilized if their rate of transfer can be stepped down to a maximum of 2400 bps (TAP specification). However, some newer modems cannot be made to transfer below 9600 bps even though you may use an initialization string that specifies a lower rate of transfer.

- **Data bits**—Select the type of data bit transmission used to communicate with the selected port (6, 7, or 8 data bits).
- **Parity**—Select the type of parity expected by the modem connected to the selected serial port.
- **Stop**—Select the stop bits used to communicate with the selected port (1 or 2 data bits).

Creating a Pager Action

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Pager Action**.
- Select an existing Pager Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter an identifying name for this pager action.
- **Description**—Enter a short description of the action. This is displayed along with the names in the Action Library.
- **Terminal number**—Enter the pager number to dial. Your service provider can provide you with this number.
- **Terminal password**—If required, enter the pager password here. This is a password that is required to log in to some paging services.
- **Modem Setup**—Select either **Primary** or one of the **Alternate** setups. Click Port Settings to further define your selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your pager notifications. There could also be times you want to change your settings to meet a specific service provider's requirements for a specific notification (for example, a lower baud rate). To do this, you can do an alternate modem setup and associate this to the notification instead of using your primary setting.

Note Changing the Port Settings for the desired modem setup will affect *all* uses of that setting.

- **Protocol**—Select the type of protocol used by your pager service.
- **Pager ID**—Enter the pager identification number.
- **Message**—Enter a text message plus any of the percent variable codes used to deliver Cisco netManager information with the page.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating an E-Mail Action

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **E-mail Action**.
- Select an existing E-mail Action, then click **Edit**.

The action properties page opens.

Step 3 Enter the e-mail destination information.

- **Name**—Enter a unique name for this action.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in the Name box.
- **SMTP Mail Server**—Enter the IP address or host (DNS) name of your e-mail server (SMTP mail host).
- **Port**—Enter the port number that the SMTP server is installed on.
- **Mail To**—Enter the e-mail addresses you want to send the alert to. Email addresses must be fully qualified. Two addresses may be entered, separated by commas (but no spaces). Addresses should not contain brackets, braces, quotes, or parentheses.

Step 4 Click **Mail Content**. Enter the content of the e-mail alert.

- **From**—Enter the e-mail address that will appear in the From field of the e-mail that is sent by the E-Mail action.
- **Subject**—Enter a text message or edit the default message. You can use any of the percent variable codes.
- **Message body**—Enter a text message or edit the default message. You can use any of the percent variable codes.

Step 5 Click **OK** to save this action. The action now appears in the Action Library.

Step 6 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Note You can also assign notifications to be sent according to device type, event type, or event severity. For more information on notifications, see Chapter 7, "Using Notifications."

Creating an SMS Action

Short Message Service (SMS) is similar to paging. However, SMS messages do not require the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability.

Note Cisco netManager transmits the SMS message to the provider, and the provider forwards it to the cell phone. Cisco netManager does not broadcast SMS messages directly.

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **SMS Action**.
- Select an existing SMS Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter a unique display name to identify the SMS notification.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in with the Name box.
- **Country**—Using the list box, select the country for the SMS provider.
- **Provider**—Using the list box, select the desired provider.

Note If the provider list is incomplete and/or incorrect, you can click the Providers button to add, edit, or delete providers in this list.

- **Connection Settings**—Mode is either Email or Dialup, depending on how the provider was created in the system.
- **Email to**—If the connection setting is Email, enter the e-mail address of the SMS device.
- **Phone Number**—If the connection setting is Dialup, enter the phone number to call with the message.
- **Message**—Enter a text message plus any desired percent variable codes.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating a Sound Action

You can add a sound to the Action library. This sound can then be assigned to an action by creating an Action Policy, or by adding an action to a specific device.

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Sound Action**.
- Select an existing WinPopup Action, then click **Edit**.

The Action Properties page opens.

Step 3 Set the appropriate options:

- **Name**—The name of the action as it appears in the Action library.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in with the Name box
- **Sound file name**—Enter the full path to the sound file, or click the folder icon to select it from your computer. The sound file name is located on the server where Cisco netManager is running.

- **Continuous play**—Select this option to have the sound play continuously until the Cancel Sound button is clicked on the main Cisco netManager toolbar.

Creating a WinPopup Action

Step 1 From the **GO** menu, select **Configure > Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **WinPopup Action**.
- Select an existing WinPopup Action, then click **Edit**.

The Action Properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter an identifying name for this winpop action.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in with the Name box.
- **Destination**—Specify the Windows NT host or domain that you want to receive this notification.
- **Message**—Enter a text message using a percent variable if needed.
- **Refresh**—Click this button to refresh the Destination list. This populates the list with all of the targets you choose to send a winpop action to.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating a Syslog Action

Step 1 From the **GO** menu, select **Configure > Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Syslog Action**.
- Select an existing Syslog Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter a name for the action. This will appear in the Action Library.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in with the Name box.
- **Syslog Server**—Enter the IP address of the machine that is running the Syslog server.
- **Port**—Enter the UDP port that the Syslog listener is listening on. The default port is 514.

- **Message**—Enter a text message to be sent to the Syslog server. This message may include notification variables. The Syslog message box limits input to 511 characters. If notification variables are used, then the message that actually gets sent will be limited to 1023 bytes, in order to comply with the Syslog protocol. Nonvisible ASCII characters such as tabs and linefeeds will be replaced by space characters.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating a Text-to-Speech Action

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Text-to-Speech Action**.
- Select an existing Text-to-Speech Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter a unique name for this action.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in with the Name box.
- **Speak Rate**—Select how fast the voice speaks the message.
- **Volume**—Select the volume of the message.
- **Message**—Enter any text message you want audibly repeated. Your own text can be used in addition to percent variables.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating a Program Action

You can define program actions to launch an external application when a state change occurs.

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Program Action**.

- Select an existing Program Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—Enter a name for the action you are creating. This is the name that appears in the Action Library.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in with the Name box.
- **Program filename**—Enter the executable name of the application you want to launch. Use the folder button to help you do this.
- **Working path**—Specify a directory where the working files for the application are stored. Use the folder button to help you do this. The working path is located on the server where Cisco netManager is running.
- **Program arguments**—Enter any percent variable you want to pass to the specified program.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating an Active Script Action

This action allows you to write either VBScript or JScript code to perform a customized action. If the script returns an error code, then the action has failed.

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Active Script Action**.
- Select an existing Active Script Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**—The name of the action as it appears in the Action Library.
- **Description**—The description of the action as it appears in the Action Library.
- **Timeout**—The amount of time (in seconds) Cisco netManager should wait for the action script to run.

Note Though the maximum timeout is 60 seconds, you should avoid using a timeout longer than the default of 10 seconds. You should use the shortest timeout possible.

- **Script type**—VBScript or JScript.
- **Script text**—Write or insert your action code here.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Creating a Web Alarm Action

A Web Alarm is an action type that plays a sound over the web interface when a device state change occurs. All users logged in via the web interface will see these alarms. The type is configured in the Actions Library, and can be associated to any device or monitor like any other action.

Step 1 From the **GO** menu, select **Configure** > **Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Web Alarms Action**.
- Select an existing Web Alarm action, then click **Edit**.

The Action Properties page opens.

Step 3 Set the appropriate options:

- **Name**—The name identifies the Web Alarm action in the Action Library list.
- **Description**—A short description of the action. The description appears in the Action Library list.
- **Message**—Enter a short message to send to the visual cue part of the Web Alarm in the web interface.
- **Play Sound**—Select this option to play the sound file whenever a web alarm action is fired. Clear this option to only have the visual cue appear in the Web Interface.
- **Sound file name**—Select a sound file that has been installed in your `the NMconsole\WebSounds` directory. Custom sounds added to this directory appear in the drop-down list.

Note For Web Alarms to work properly, your browser must support embedded sound files.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Dismissing or Muting Web Alarms

A dialog appears in the web interface when one or more of these alerts fire. This dialog allows you to dismiss or mute the alarms that have been fired. Clicking the Dismiss or Dismiss All button stops only the current sound being played. It does not stop the sound for future occurrences of the Web Alarm. To disable Web Alarms, go to **Configure** > **Preferences** and clear the Enable web alarms option.

When you double-click an entry in this dialog, you are taken to that device's Device Status report.

Creating a Service Restart Action

After you configure this action, you can start or stop an NT service when another device or monitor experiences a state change. In order for the Service Restart Action to work:

- Both the Cisco netManager computer and the target device (where NT service is to restart) must have identical user accounts.
- The Cisco netManager Engine service needs to log in as a user account that belongs to the administrators group and that exists on the target machine.

Step 1 From the **GO** menu, select **Configure > Action Library**.

Step 2 In the Action Library, do one of the following:

- Click **New**, then select **Service Restart Action**.
- Select an existing Service Restart Action, then click **Edit**.

The action properties page opens.

Step 3 Set the appropriate options:

- **Name**.—Enter the name of the action as you would like it to appear in the Action Library.
- **Description**—Enter a short description of the action. This is displayed in the Action Library along with the entry in the Name box**.**
- **Host—**Click the browse button to select the desired host from your Network Neighborhood.
- **User name (domain\username)**—Enter a user login to use with this monitor. To monitor the service on another machine, the WinEvent monitor has to be configured with the correct user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, then the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user. No user name or password is needed for local services (services on the machine where Cisco netManager is running).
- **Password**—Enter the password for the login used above. To monitor NT services on an XP machine with an account that has no password, the XP's Local Security Settings might have to be modified. From **Administrative tools** > **Local Security Settings**, click **Security Settings** > **Local Policies** > **Security Options**. Then right click the setting **Account: Limit local account use of blank passwords to console logon only** and click **Properties**, then select **Disable**.
- **Service**—Click the browse button to select the desired service associated with your host.
- **Command**—Use the list box to select either Start or Stop, depending on whether you want the associated alert to Start or Stop the service you have selected.

Step 4 Click **OK** to save this action. The action now appears in the Action Library.

Step 5 Assign the action to a device or a monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Configuring Recurring Actions

This feature gives users the ability to execute actions based on a regular schedule, independently of the status of devices. Among other things, this can be used to send regular *heartbeat* messages to a pager or cell phone, letting the user know the system is up and running.

After an action has been configured through the Action Library, use this feature to configure the schedule for the action. The recurring action list shows the name of the action and the recurring schedule configured for that action.

Note Recurring actions can be configured to adhere to a blackout schedule.

Step 1 From the GO menu, select **Configure** > **Recurring Actions...**.

Step 2 Do one of the following:

- Click **New** to create a new recurring action.
- Select an entry and click **Edit** to make changes that entry.
- Select an entry and click **Copy** to create a copy of that entry. You can then edit the new copy as needed. GO to Step 4.

Step 3 Enter the following information:

- **Action name**—Enter a name for the recurring action.
- **Select an action**—Select an action from the drop-down list. This list displays all actions in your Action Library that you can configure as the recurring action.
- Click **browse (...)** next to the Select an action box to launch the Action Library. In the Action Library, you can create a new action to configure as the recurring action.

Note A Web Alarm action cannot be used as a recurring action.

Step 4 Enter the following information:

- **Enable this schedule**—Select this option to activate the recurring action; clear the option to disable the recurring report.
- **Blackout Schedule**—Click this button to access the Weekly Blackout Schedule dialog box.
- **Monthly**—Select the time, day, and month or months you want the action to execute. The action only executes during the month selected from this list. Quarterly actions can be created by selecting the last day of each quarter. If a day is entered that does not exist in a selected month (September 31, February 30, and so on) then the action is executed on the last day of that month.
- **Weekly—**Select the day and time each week you want the action to execute.

To execute an action more frequently than daily, select **Every _minutes** and enter a number of minutes for Cisco netManager to wait before firing the recurring action.

Note To schedule multiple time periods, you must create another recurring action.

Step 5 Click **Finish**.

Testing an Action

After an action has been created, you can test that action to make sure it works properly.

To test an action:

Step 1 Select **Configure > Action Library**. The Action Library appears.

Step 2 In the Action Library, select the action you want to test.

Step 3 Click **Test**.

Step 4 Review the action in the Action Progress dialog.

Deleting an Action

To remove actions that were added at the device or monitor level, select the action in the Actions dialog of the Device or Monitor Properties, and click **Remove**. This does not effect any other item in the database.

If you have assigned action policies to your devices, you can remove the action from the policy itself.

To completely remove an action from the database, you must access the Action Library, select the action and click **Delete**. When an action is removed from the Library, it is also removed from all items configured to use that action.

Assigning an Action to a Device

You can assign one or more individual actions to a device, or assign an action policy that may contain multiple actions used across your device list.

To assign actions to a device:

Step 1 Right-click a device, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Actions**. The Actions dialog opens.

Step 3 Select the **Apply individual actions** option.

Step 4 Click **Add** to access the Action Builder wizard.

Step 5 Follow the directions in the Action Builder wizard.

Step 6 At the end of the wizard, click **Finish** to add the action to the device.

Step 7 If you need to add more actions to the device, click **Add** and repeat these directions.

Step 8 When you have completed adding actions, click **OK**.

To assign an action policy to a device:

Step 1 Right-click a device, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Actions**. The Actions dialog opens.

Step 3 Select the **Apply this Action Policy** option.

Step 4 Select the action policy you want to use for this device. If you need to create a new action policy first, click **Add** to access the Action Builder dialog.

Step 5 Click **OK** to save the changes.

After an action has been added to the device, the action fires when that device reaches the specified state.

Assigning an Action to a Monitor

You can assign one or more individual actions to a monitor, or assign an action policy that may contain multiple actions.

To assign an action to an active monitor:

Note During the configuration of a new monitor, you are presented with the Action Builder as part of the wizard. The following set of directions is for existing monitors.

Step 1 Right-click the device the active monitor is configured on, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Active Monitors**. The Active Monitors dialog opens.

Step 3 Double-click the monitor you want to add actions to.

Step 4 Do one of the following to go to the Actions Properties page:

- In the web interface, in the Active Monitor Properties wizard, click **Next**.
- In the console, in the Active Monitor Properties dialog, select **Actions**.

Step 5 Select the **Apply individual actions** option.

Step 6 Click **Add** to access the Action Builder wizard.

Step 7 Follow the directions in the Action Builder wizard.

Step 8 At the end of the wizard, click **Finish** to add the action to the monitor.

Step 9 If you need to add more actions to the monitor, click **Add** and repeat these directions.

Step 10 Click **OK** after all actions have been added.

To assign an action policy to an active monitor:

Note During the configuration of a new device, you are presented with the Action Builder as part of the wizard. The following instructions are for existing devices.

Step 1 Right-click the device the active monitor is configured on, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Active Monitors**. The Active Monitors dialog opens.

Step 3 Double-click the monitor you want to add actions to.

Step 4 Do one of the following to go to the Actions properties dialog box:

- In the web interface, in the Active Monitor Properties wizard, click **Next**.
- In the console, in the Active Monitor Properties dialog, select **Actions**.

Step 5 Select the **Apply this Action Policy** option.

Step 6 Select the action policy you want to use for this device. If you need to create a new action policy first, click the browse button to access the Action Policies dialog.

Step 7 Click **OK** to save the changes.

To assign an action to a passive monitor:

Step 1 Right-click the device the passive monitor is configured on, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Passive Monitors**.

Step 3 Double-click the monitor you want to add actions to. The Passive Monitor Properties page opens.

Step 4 Click **Next**.

Step 5 Click **Add** to access the Action Builder wizard.

Step 6 Follow the directions in the Action Builder wizard.

Step 7 At the end of the wizard, click **Finish** to add the action to the monitor.

Step 8 If you need to add more actions to the monitor, click **Add** and repeat these directions.

Step 9 Click **OK** after all actions have been added.

Note You cannot assign an action policy to a passive monitor.

After an action has been added to the monitor, the action fires when that state reaches the assigned down state.

Creating a Blackout Period

You can create a blackout period to have Cisco netManager suspend specific actions during the scheduled period of time. Use this feature to keep from sending a notification to someone who is on vacation, or to keep from sending e-mail when there is no one to receive it.

To create a blackout period:

Step 1 Access the Action Builder Wizard.

Step 2 Within this wizard, click the **Blackout period** button.

Step 3 On the Weekly Blackout Schedule dialog, set the times you want the blackout to occur. The schedule that is set is repeated weekly.

Step 4 Click **OK**.

Step 5 Complete the wizard.

About Percent Variables

Table 6-1 Active Monitor Variables

Active Monitor Variables	Description
%ActiveMonitor.Argument	SNMP instance number. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.Comment	The human readable name that coincides with the network switch. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.Name	The name of the active monitor that fired an action. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.NetworkInterfaceAddress	IP address for the network interface. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.Payload	The payload returned by a WMI, Exchange, SQL, or SNMP active monitor. This is only used when an action is associated directly with an active monitor and not the device as a whole.
%ActiveMonitor.State	The current status of the monitor, such as "Down at least 5 min." This is only used when an action is associated directly with an active monitor, and not the device as a whole.

Table 6-2 Device Variables

Device Variables	Description
%Device.ActiveMonitorDownNames	List of down services using the abbreviated name if available.
%Device.ActiveMonitorUpNames	Full service names of all monitored services on a device with an up status.
%Device.Address	IP address (from the device properties page).

Table 6-2 Device Variables (continued)

Device Variables	Description
%Device.Attribute.[Attribute Name]	Returns an attribute from the SNMP information available for the device, such as the contact name. To specify the attribute, append the category name (listed below) to the end of the variable. For example: `%Device.Attribute.Contact`, returns the contact name. Default categories: • *. Returns all attributes. • Info1. Upgrade path from v8. • Info2. Upgrade path from v8. • Contact. Contact information from SNMP. • Location. Location information from SNMP. • Description. Description information from SNMP. • Custom. If you have created a custom attribute you can use the name of that custom attribute in the percent variable. Example: %Device.Attribute.Phone %Device.Attribute.RackPosition To avoid an error, when placing %Device.Attribute in quotation marks, place a space between the last letter and the closing quotation mark. Example: "%Device.Attribute.Contact" (correct) "%Device.Attribute.Contact" (incorrect)
%Device.DatabaseID	Returns the database ID of a device.
%Device.DisplayName	Display Name (from the General section of the device properties page).
%Device.HostName	Host Name (from the General section of the device properties page).
%Device.Notes	Notes. (from the Notes section of the device properties page).
%Device.SNMPOid	SNMP object identifier.
%Device.State	The state's description (such as "Down at least 2 min" or "Up at least 5 min").
%Device.Status	The name of the active monitor, preceded by the device state ID; for example, 10|DNS.
%Device.Type	Device Type (from the General section of the device properties page).

Table 6-3 Passive Monitor Variables

Device Variables	Description
%PassiveMonitor.DisplayName	The name of the monitor as it appears in the Passive Monitor Library.
%PassiveMonitor.LoggedText	Detailed event description: • SNMP traps—Returns the full SNMP trap text. • Windows Log Entries—Returns information contained in the Windows Event Log entries. • Syslog Entries—Returns the text contained in the Syslog message.
%PassiveMonitor.Payload.*	Payload generated by a passive monitor.
%PassiveMonitor.Payload.EventType	The type of passive monitor (Syslog, Windows Event, or SNMP Trap).

Table 6-4 System Variables

System Variables	Description
%System.Date	The current system date. Configure the date format in Regional Options (from Program Options).
%System.DisplayNamesDownDevices	Displays names of devices with down monitors.
%System.DisplayNamesDownMonitors	Shows the name of a device and each monitor that is down on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping
%System.DisplayNamesUpDevices	Displays names of up devices.
%System.DisplayNamesUpMonitors	Shows the name of a device and each monitor that is up on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping
%System.InstallDir	Displays the directory on which Cisco netManager is installed.
%System.NumberofDownDevices	Number of down devices on your network.
%System.NumberOfDownMonitors	Number of down monitors on your network.
%System.NumberofUpDevices	Number of up devices on your network.
%System.NumberOfUpMonitors	Number of up monitors on your network.
%System.Time	The current system time. The format is hh:mm:ss.

About Action Policies

You can use Action Policies to stack multiple actions together in a single policy. You can then assign the action policy to any device or monitor. If you later need to edit an action, you can edit the action policy and the changes will be applied to all of the devices that use that particular action.

The Action Policy dialog shows the action policies that you can assign to any device or monitor. This is where you create a new action policy, modify an existing policy, or delete a policy.

To open the Action Policies, from the menu bar:

Step 1 Select **Configure** > **Action Policies**.

Step 2 From this dialog, you can:

- **Create a new policy**—Click New. Use the Add/Edit Action Policy dialog to create a policy.
- **Change an existing policy**—Select the policy you want to change and click Edit. Use the Add/Edit Action Policy dialog to edit the policy.
- **Copy an existing policy**—To create a copy of an action policy so you can base a new policy on the setup information of an existing one, select the action policy and click Copy. You can then edit the new copy as needed.
- **Remove a policy**—Select the policy you want to remove and click Delete. This deletes the policy and removes it from use on any devices or monitors to which it is assigned, though it does not remove the actions configured under the policy. Also, any record in the Action Log for this action policy is deleted.

For more information, see:

- Creating an Action Policy, page 6-21
- Editing Action Policies, page 6-22
- Implicit Action Policy, page 6-22

Creating an Action Policy

This feature gives you the ability to stack multiple actions together in a single policy. You can then assign those actions to any device or monitor in your device list. Once assigned, you can edit the policies in the Action Policies dialog without having to make changes to all of the devices that use that particular action.

To create an action policy:

Step 1 From the menu bar, select **Configure** > **Action Policies**. The Action Policies dialog opens.

Step 2 On the Action Policies dialog, click **New**.

Step 3 In the New Action Policy dialog, enter a name in the Policy name box. This name is used to identify the policy later, so you should make sure the name is something that will help you remember what is contained in that policy.

Step 4 Click **Add**. The Action Builder wizard appears.

Step 5 Follow the directions in the wizard.

Step 6 Click **Finish** at the end of the wizard to add the action to the policy.

Step 7 Add as many actions as you need to complete the policy. To move actions up and down in the list, click the **Up** and **Down** buttons above the action list.

If you select Only execute first action, Cisco netManager executes the actions in the list, starting at the top, and stops as soon as an action successfully fires.

Step 8 Once all of the actions have been added, click **OK** to create the policy and add it to the active list.

Step 9 Assign the action policy to a device or monitor by using the procedure defined in:

- Assigning an Action to a Device, page 6-15
- Assigning an Action to a Monitor, page 6-16

Note During device discovery, you can assign an existing action policy (if one has been created previously), create a simple action policy through a wizard, or access the Action Policy Editor to create an action policy yourself.

Editing Action Policies

When you make changes to an action policy, you change the operation of all items that are currently assigned to use the policy.

To edit an action policy:

Step 1 From the main menu, select **Configure > Action Policies**. The Action Policies dialog opens.

Step 2 On the Action Policies dialog, select the policy you want to edit.

Step 3 Click **Edit**.

Step 4 Make changes to the policy as necessary.

Step 5 Click **OK.**

Implicit Action Policy

With the Implicit Action Policy, Cisco netManager automatically assigns actions to all devices in your database. There is no way to opt out of the Implicit Action policy, so any action in that policy will be used by all devices. The Implicit Action Policy is not used for active monitors, just devices.

The Implicit Action policy is configured and can be edited through the Action Policies dialog. If at any time during the normal operation of Cisco netManager you notice that actions are firing and you cannot find the action associated to the down device or monitor, remember to check the Implicit Action Policy.

About Acknowledgements

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 a state change occurred. In the device list, the name of the device appears in bold, and in the map view, the device name appears on a black background.

After the device is placed in Acknowledgement mode, it remains in this mode until you actively acknowledge it.

Acknowledging a device state change does not keep that device from firing actions. To stop a device from firing actions, you must put the device into maintenance mode.

To acknowledge a state change, do one of the following:

- Select the device or devices you want to acknowledge and right-click a selected item. In the right-mouse menu, select **Acknowledge**.
- Access the State Change Acknowledgement report and select the devices you want to acknowledge. After the devices are selected, click **Clear** to remove the devices from the report, thereby acknowledging the state change.

Example: Getting an E-Mail Alert when the Web Server Fails

This example shows how to set up monitoring of your web server so that you get an e-mail alert when the web server fails, or when web content is not available.

First, you need to set up the monitors for your web server. Then, create an e-mail action and assign it to the monitors. Both tasks can be done within a wizard.

Step 1 Open device properties for your web server device, then select the Active Monitor properties.

Step 2 Click **Add**. The Active Monitor Properties wizard opens.

Step 3 Use the wizard to add the HTTP active monitor to your web server device. This monitor verifies that HTTP (port 80) is active.

a. On the Select Active Monitor Type screen, select **HTTP**, then click **Next**.

b. On the Set Polling Properties screen, click **Next**.

c. On the Setup Actions for Monitor State Changes screen, select **Apply individual actions**, then click **Add**.

d. On the Select or Create Action screen, select **Create a new action**, then click **Next**.

e. On the Select Action Type screen, select **E-Mail Action**, then click **Next**.

f. On the Select State Change screen, click **Finish**.

g. On the New Email Action screen, enter the information.

h. Click Mail Content, enter the information.

i. Click **OK** to save changes and return to the previous screen. Click **OK** again to return to the Setup Actions for Monitor State Changes screen. Click **Finish**.

Step 4 Use the same wizard to add the HTTP Content active monitor. This monitor verifies that the web server returns some valid content in response to an HTTP request.

a. On the Select Active Monitor Type screen, select **HTTP Content**, then click **Next**.

b. On the Set Polling Properties screen, click **Next**.

c. On the Setup Actions for Monitor State Changes screen, select **Apply individual actions**, then click **Add**.

d. On the Select or Create Action screen, select **Select an action from the Action Library**, then click **Next**.

e. On the Select Action and State screen, select **MailtoWebmaster**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes screen.

f. Click **Finish**.

The two active monitors and resulting e-mail action are now enabled. When the web server is down for more than 2 minutes, HTTP active monitor will fail, triggering the e-mail action.

Note You can also assign notifications to be sent according to device type, event type or event severity. For more information on notifications see Chapter 7, “Using Notifications.”

CHAPTER 7

Using Notifications

Cisco netManager captures events that occur in the Unified Communications environment and the IP fabric. Cisco netManager can send e-mail notifications each time a new event is found. E-mail notifications can be filtered based on rules that specify the device type, event type, or event severity.

See the following topics for more information on notifications:

- Notification Filtering, page 7-1—Explains the concept of notification filtering.
- Configuring Notifications, page 7-2—Provides information on how to configure notification criteria.
- Managing Notifications, page 13-9—Provides system registry information on notification configuration options:
  - Performance and E-Mail Details, page 13-9
  - Configuring SMTP Load, page 13-9
  - Configuring Socket Timeouts, page 13-10
  - Notification Logging, page 13-10

Note Some antivirus programs automatically scan outgoing e-mail which can affect performance. See the appropriate antivirus product documentation to disable this option.

In addition to sending e-mail notifications, you can configure Cisco netManager to initiate actions (depending on the responses received from polling, or the types of messages received) to notify you of any change on your network. You can configure actions on a single device or monitor, or define an Action Policy to use across multiple devices or monitors. For more information on actions, see Chapter 6, “Using Actions.”

Notification Filtering

You can set notification rules that dictate what type of events are sent and to whom they are sent. You can do the following with notifications:

- Create multiple rules based on:
  - Devices
  - Groups
  - Event types

  - Event severity
- Specify multiple SMPTP servers and multiple recipients
- Filter out duplicates of the same event

For each event, Cisco netManager compares the event type, device type, and severity against the user-configured notification rule and sends a notification when there is a match. The procedure for configuring notification criteria is described in Configuring Notifications, page 7-2.

What Are Notification Criteria?

Notification criteria define what you want to monitor for the purpose of sending notifications. A notification criterion is a user-defined, named set of devices or phones, and alerts and events of a particular severity. You must specify device-based notification criteria to configure a notification group.

  - Devices—The devices or device groups that you want to monitor.
  - Event groups—(Optional) One or more types of events that you want to monitor.
  - Event severity—(Optional) One or more event severity levels.

Limiting Notifications to Those for Specific Events

In some cases, you might want to send notifications for only a subset of the events that Cisco netManager monitors. You can select a group of events and/or specify the severity of events for which you want to send notifications. You can define this criteria to:

- Limit the number of events that Cisco netManager notification monitors.
- Aggregate the notifications that you want to send to different destinations. For example, you can create separate event groups to limit the number of e-mail notifications sent to specific individuals or departments.

Configuring Notifications

From **GO** > **Notification Settings**, you can configure Cisco netManager to send e-mail notifications when specific events occur on specific device groups.

Note Some antivirus programs automatically scan outgoing e-mail which can affect performance. See the appropriate antivirus product documentation to disable this option.

From this page you have the following options:

- **New**—Creates a new notification group.
- **Edit**—Modifies the selected notification group.
- **Copy**—Copies a selected notification group that you can later edit. You can use existing notification groups as templates for creating new notification groups; for example, to create a new notification group with the same list of e-mail addresses of an existing notification group.
- **Delete**—Deletes the selected notification group.

- **View**—Displays the Notification Summary page, where the configuration information for a notification group is displayed.

These topics explain the activities you can perform from the Notifications page:

- Adding and Editing Device Notification Rules, page 7-3
- Cloning a Notification Rule, page 7-4
- Viewing Notification Rule Configuration Details, page 7-5
- Deleting Notification Rules, page 7-5

Adding and Editing Device Notification Rules

This topic describes the procedures for adding or editing a device notification group.

Note Some antivirus programs automatically scan outgoing e-mail which can affect performance. Please see the appropriate antivirus product documentation to disable this option.

Step 1 Select **GO** > **Configure** > **Notifications Settings...**.

Step 2 Do one of the following:

- To add a new criterion, click **New...**.
- To edit an existing criterion, select the notification group and click **Edit...**.

Step 3 Edit the information on the page, described in the following table.

Table 7-1 Notification Criterion

GUI Element	Description/Action
Notification Name	Descriptive name for the notification.
IPv4 Address of SMTP Server	Enter a fully qualified IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.)
Recipient E-Mail Address(es) separated by comma, semicolon, or space	Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon. If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.

Step 4 Click **Next**. The Add Notification — Device Group page appears.

Step 5 Check one of the following:

- **Select all devices**—Includes all devices in this notification.
- **Select devices or device groups**—Includes devices and device groups that you select to include in this notification. Expand device group folders and select check boxes for one or more devices or device groups.

Note

- If you select a device group, the notification criterion will stay up-to-date when individual devices are added or deleted from the device group. However, if the device group is deleted, the group is removed from all notification rules. You will have to configure the notification criterion again even if the same device group is added back with the same name.
- If you select an individual device, and the device is deleted later, the notification criteria is also deleted.You will have to configure the notification criterion again even if the device is added back later.
- All events present in the devices you select can be included in this notification using the next wizard screen.

Step 6 Click **Next**.The Add Notification—Events page appears.

Step 7 Check one of the following:

- **Select all events**—Includes all events associated with the devices selected in the previous screen.
- **Select group of events**—Includes events that you select to include in this notification. Expand event group folders and select check boxes for one or more events or event groups.
- Select none, one, or more of the following:
  - Critical.
  - Warning.
  - Informational.

Step 8 Click **Next**. The Notification Group Summary page appears, displaying all information entered on the previous page.

Step 9 Click **Finish**. The notification information is saved.

Note You can use existing notification groups as templates for creating new notification groups. For procedures, see Cloning a Notification Rule, page 7-4.

Cloning a Notification Rule

You can use existing notification rules as templates for creating new notification groups.

Step 1 Select **GO** > **Configure** > **Notifications Settings...**.The Notification page appears.

Step 2 Select notification group that you want to use as the base for your new notification group.

Step 3 Click **Close**.

The rest of the procedures for cloning a notification rule are the same as for editing a notification group. For further instructions, see Adding and Editing Device Notification Rules, page 7-3.

Viewing Notification Rule Configuration Details

Step 1 Select **GO** > **Configure** > **Notifications Settings...**.The Notification rules page appears.

Step 2 Select the notification group that you want to view.

Step 3 Click **View**. The Notification Group Summary page appears, displaying the following information:

- Notification Name.
- Notification Group Details—SMTP server, SMTP port, recipient e-mail addresses.
- Device Details—Selected devices for this notification.
- Event Details—Selected events and any applicable event severity types (critical, warning, or informational).

Deleting Notification Rules

Step 1 Select **GO** > **Configure** > **Notifications Settings...**.The Notification Groups page appears.

Step 2 Select the notification group that you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes** to confirm.

CHAPTER 8

Using Active Monitors

Active Monitors query network services installed on a device, then wait for the response. If a response is not received or if the response does not match what is expected, the service is considered down, and a state change occurs on the device. If the query is returned with the expected response, the service is considered up. The following active monitor types are available in Cisco netManager:

- DNS Monitor
- NT Service Monitor
- Ping Monitor
- Active Script Monitor
- SNMP Monitor
- TCP/IP Monitor
- Telnet Monitor

Note There are several types of TCP/IP Monitors that are configured using the same dialog box.

About Monitors and Actions

The monitors and the action systems work together in Cisco netManager to help you stay informed about what is happening on your network and the devices connected to your network. It is a cooperative relationship that can be configured to go well beyond the default setting included with the installation of the product. With some helpful examples and some creativity, a network administrator should be able to tailor the monitors and actions systems to watch over all of their important devices and troubleshoot problems that may arise.

Using Monitors and Actions

When you set up actions and monitors, keep in mind the following, to help you maximize the usefulness of the features and minimize problems.

- **Action Coverage**. Set up your notification actions so that the people who have to be notified are sent the alert. Consider creating vacation action types that will not send alerts to people who cannot do anything about it.
- **Understanding SNMP**. It will take a little research, but when you find out which of your network devices have SNMP capabilities, you can configure monitors to listen for all types of information and trigger an Action accordingly.
- **Security Features**. Pay careful attention to the devices and services that are critical to your network security.
- **Network Resources**. Configure Cisco netManager to perform an action when your network resource availability diminishes across a certain threshold.
- **Assigning Actions to Devices or Monitors**. Assign actions to the device if you only want one notification when the device goes down. Assign an action to a specific active monitor if it requires special attention.

About the Active Monitor Library

The Active Monitor Library is the central storehouse of all active monitors that have been configured for your network. When changes are made to the active monitors listed in this dialog box, the changes affect each instance of that particular monitor across your device groups.

Access the Active Monitor Library from the main menu of the Cisco netManager. In the web interface, click **GO** > **Configure** > **Active Monitor Library**.

This dialog box is used to configure new or existing active monitor types. The list shows all types currently configured for use in Cisco netManager. From here, you can do the following:

- To configure a new active monitor type, click **New**.
- To change the current configuration of an active monitor type, select an existing type, then click **Edit**.
- To make a copy of that type and add it to the list, select an active monitor type, then click **Copy.**
- To remove an active monitor type, select it from the list, then click **Delete**.
- In the Cisco netManager console, you can select an active monitor, then click **Test** to test the selected active monitor on a device.

Supported Active Monitor Types

The following is a list of all of the active monitor types that are supported by Cisco netManager:

- **Active Script Monitor**—The Active Script Monitors let you write either VBScript or JScript code to perform a check on a device. If the script returns an error code, the monitor is considered down.

Note Cisco netManager does not support the scripts that you create, only the ability to use them in the Active Script Monitor.

- **DNS Monitor**—The DNS monitor checks for the Domain Name Server (DNS) on port 53. If no DNS service responds on this port, then the service is considered down.

- **SNMP Monitor**—Simple Network Management Protocol is the protocol governing network management and monitoring of network devices and their functions. This monitor queries the SNMP device and tries to match the expected returned value.
- **Telnet Monitor**—Telnet is a simple service monitor that checks for a Telnet server on port 23. If no Telnet service responds on this port, then the service is considered down.
- **Ping Monitor**—The Ping Monitor sends an ICMP (ping) command to the device. If the device does not respond, the monitor is considered down.
- **TCP/IP Monitor**—The TCP/IP Monitor is used to monitor a TCP/IP service that either does not appear in the list of standard services or uses a nonstandard port number.
- **NT Service Monitor**—The NT Service Monitor lets you check the status of a service on a Windows machine and attempts a restart of the service (if the appropriate Administrator permissions exist).

Note A running Windows Management Instrumentation (WMI) service on the targeted machine is required for this NT Service Monitor to work properly. Windows 2000 Service Pack 2 or higher, XP, and 2003 are installed with the WMI service. WMI is not installed with Cisco netManager, but can be downloaded from Microsoft and installed on Windows NT.

Assigning Active Monitors

There are two steps in assigning an active monitor to a device. The first is to configure the active monitor in the Active Monitor Library, and the second is to add that monitor to a device. For most users, the default configuration is sufficient and there is no need to make any changes to the active monitors in the library.

To configure an active monitor:

Step 1 From the web interface main menu, select **GO > Configure > Active Monitor Library** to view the Active Monitor Library.

Step 2 Do one of the following:

- Click **New** to configure a new active monitor.
- Select a monitor from the list and click **Edit** to make changes to an existing configuration.

Step 3 After you make the necessary changes, click **OK** to add the monitor to the list, or to save the changes you made to one already on the list.

To add an active monitor to a device:

Step 1 Select the active monitors you want to scan for during Device Discovery. When you select the discovered devices and add them to your database, Cisco netManager creates a monitor for each network service found.

Step 2 In the Device Properties Active Monitor dialog box, click **Discover**. Cisco netManager scans the device and creates a monitor for each network service found.

Step 3 Manually assign an active monitor to the device:

a. In the Device Properties Active Monitor dialog box, click **Add**. The Active Monitor Properties dialog box opens.

b. Select the active monitor type you want to assign to the device, then click **Next**.

c. Set the polling properties for the monitor, then click **Next**.

d. Setup actions for the monitor state changes.

e. Click **Finish** to add the monitor to the device.

Step 4 Add a new device. Click **GO** > **Devices** > **New Device**. The Add New Device dialog box opens.

Step 5 Click **Advance**. The Device Discovery Properties dialog box opens.

Step 6 In the **Select Active Monitors to be used in the scan process** section, select the active monitor types you want to assign to the device.

Step 7 Click **OK**.

Step 8 Use **Bulk Field Change** to add an active monitor to multiple devices:

a. Select the devices in the device list, then right-clicke of the selected items.

b. From the right-mouse menu, select **Bulk Field Change** > **Active Monitor**.

c. Select the active monitor type you want to add.

d. Click **OK**.

Deleting Active Monitors

Unless you are absolutely sure you need to remove an active monitor type from the Active Monitor Library, you should never have to delete an item from this list. If you do, and you find you need it later, you will have to reconfigure it completely, including the default types that were added during initial installation of Cisco netManager. We recommended that you only delete the custom monitors that you create.

Caution When you remove an active monitor type from the library, all active monitors of that type are deleted from the devices you are monitoring, and all related report data is lost.

The best course of action is to remove the monitors at the device level or to disable the monitor by clearing the selection on the Device Properties.

To remove a monitor from a device:

Step 1 Right-click the device you want to remove the monitor from, then click **Properties**. The Device Properties dialog box opens.

Step 2 Click **Active Monitors**. The active monitors attached to the selected device displays in the list.

Step 3 Select the monitor you want to remove.

Step 4 Click **Remove**. A warning dialog box opens, stating that all data for that monitor will be deleted if the monitor is removed.

Step 5 Click **Yes** to remove the monitor.

Note If you want to stop monitoring an active monitor on a device, but want to keep the historical data, then you must disable the monitor instead of deleting it from a device.

Using the Bulk Field Change Feature

To remove an active monitor from multiple devices:

Step 1 Select the devices in the Device View or Map View, then right-click one of the selected items. The context menu opens.

Step 2 Select **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog box opens.

Step 3 In the **Operation** list, click **Remove**.

Step 4 In the **Active Monitor type** list, select the active monitor that you want to remove.

Step 5 Click **OK** to remove the monitor from the selected devices.

Group and Device Active Monitor Reports

The following reports display information for devices or device groups that have active monitors configured and enabled. Access these reports from the Reports tab on the web interface.

- State Change Acknowledgement
- Active Monitor Availability
- Active Monitor Outage
- Health
- State Change Timeline
- State Summary
- Device Status

Example: Monitoring Network Printer Toner Levels

To avoid running out of printer ink in the middle of print jobs, or wasting toner by switching toner cartridges before they are empty, through Cisco netManager you can create a custom SNMP active monitor that will notify you when toner levels are low.

To configure the printer monitor:

Step 1 From the Cisco netManager web interface, click **GO > Configure > Active Monitor Library**. The Active Monitor Library dialog box opens.

You need to create an active monitor for each printer type in use. It may be that the office uses the same printer type in each office. In this example, we are using a Hewlett Packard LaserJet 4050N. Check your network printers for their specific maximum capacity toner levels.

Step 2 Click **New**, select **SNMP Monitor**, then click **OK**. The Add SNMP Monitor dialog box opens.

Step 3 Enter a Name and Description for the monitor; for example, TonerMonitor and Toner monitor for the Hewlett Packard LaserJet 4050N.

For the **Object ID** and **Instance**, click the browse (**...**) button; then locate and find the **prtMarkerSuppliesLevel (OID 1.3.6.1.2.1.43.11.1.1.9) SNMP** object in the MIB object tree. This SNMP object is found in the MIB tree at:

```
- mgmt
  - mib 2
      - printmib
          - prtMarkerSupplies
          - prtMarkerSuppliesEntry
          - prtMarkerSuppliesLevel
```

Step 4 Select **Range of Values** from the drop-down menu and enter 4600 (the maximum capacity toner level) as the high value and 100 as the low value, then click **OK**. The action will fail when the printer toner level reaches 99.

Step 5 Test the newly created active monitor and make appropriate changes, if needed.

Step 6 Assign the active monitor to the printer device by clicking **Device Properties > Active Monitors**.

Step 7 In the Active Monitor dialog box, click **Add**.

Step 8 During the configuration wizard, create or select an action to notify you when the printer’s toner levels are low.

Step 9 Repeat steps 6 through 8 for each network printer that requires monitoring.

Expression Editor

Cisco netManager knows the proper connecting commands for checking the standard services listed on the Services dialog box, but to monitor a custom service, you may want to specify what commands to send to the service and what responses to expect from the service in order for Cisco netManager to consider the service up. It is up to you to determine the proper command strings to expect and send for a custom service.

You can use a rule expression to test a string of text for particular patterns.

Script Syntax

You create a script using keywords. In general, the Script Syntax is **Command=String**. Command is either **Send**, **Expect**, **SimpleExpect** or **Flow Control**.

Note A script can have as many send and receive lines as needed. However, the more you have, the slower the service checking.

Keywords

- To send a string to a port, use the Send= keyword.
- To expect a string from a port, use the SimpleExpect= or the Expect= keyword.
- To comment out a line, use the # symbol as the first character of the line.
- To have conditional responses on "error" or "success" of a step within the scripts, use Flow Control Keywords.

Examples

You have a TCP service to check, where you need to do the following:

- Expect something on connection
- Send a command
- Check for a response
- Send something to disconnect

Script Syntax: Expect=Keyword

This keyword provides you a great amount of flexibility to accept variable responses and choose only the information you need. This is accomplished using special control characters and regular expressions. If you do not need all this flexibility or are new to writing your own custom TCP/UDP scripts, then you may want to start off using the SimpleExpect keyword first.

Variations of the Expect Keyword

There are four variations of the Expect keyword:

- **Expect**. Returns true when the expected value is matched.
- **Expect(MatchCase)**. Returns true only when the case matches the expected value.
- **DontExpect**. Returns true when the value is not found.
- **DontExpect(MatchCase)**. Returns true when the value is not found.

The Expect syntax has the form `Expect=Response` where the Response is specified either as an exact text string or as a mixture of regular expression rules and text. The Add/Edit Expect Rule button will help you construct and test a regular expression response string. It will automatically choose the variation of Expect for you based on options you select in that dialog box. The Add/Edit Expect Rule button does not aid in the generation of SimpleExpect keywords.

Note The `~`, `^`, `!` and `=` = codes have been replaced with variations on the Expect keyword itself. Migrated definitions will be converted automatically.

```
Example 1:
#
# Note: script comments start with a # character
```

```
#
# Send a simple text command
#
Send = Hello There
#
# Expect a nice response that begins with, "Hi, How are you"
#
Expect=^Hi, How are you

Example 2:
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
#
# Expect a large response, but we only care to check that somewhere
# in the response John Doe is mentioned
#
Expect=John Doe

Example 3:
#
# Send a binary escape (27) and an x y and z and then a nak (21)
#
Send=\x1Bxyz\x15
#
# Expect something that does *not* contain 123 escape (27)
#
DontExpect=123\x1B
```

Script Syntax: Flow Control Keywords

The script language has been expanded to have conditional responses on "error" or "success" of a step within the scripts. This is done by using the following keywords:

- **IfState**. Checks for the current state (ok or error) and jumps to a label if true.
  Valid syntax: `IfState {ERR|OK} label`
  Example:
  `IfState ERR End`
  `IfState OK Bye`
- **Goto**. This immediately jumps to a label.
  Valid syntax: `Goto End`
  Example:
  `Goto End`
- **Exit**. This immediately ends the script with an optional state (ok or error). The optional state overrides the current state.
  Valid syntax: `Exit {ERR|OK}`
  Example:
  `Exit ERR`
  `Exit OK`
- **:Label**. This defines a label that can be the target of a jump. A label is defined by a single word beginning with the ":" character.
  Valid syntax: `:`(with a name following)
  Example:
  `:Bye`

- **OnError**. This allows for a global handling of an error situation.
  Valid Syntax: `OnError {EXIT|CONTINUE|GOTO} label`

  Example:
  ```
  OnError EXIT (Default behavior)
  OnError CONTINUE
  OnError GOTO Logoff
  ```

Script Syntax: Send=Keyword

To send a command on a connection, use a Send=keyword. The form is Send=Command. The command is exactly the message you want to send. You may use a combination of literal characters and binary representations.

Cisco netManager understands the C0 set of ANSI 7-bit control characters. A binary can be represented as `\x##`, where ## is a hexadecimal value. Those familiar with the table may also choose to use shorthand such as `\A (\x01)` or `\W (\x17).`

You can use `\r` and `\n` as the conventions for sending the carriage return and line feed control characters to terminate a line.

The following table shows the keywords you can use.

Keyword	Description
\x##	Binary value in hexadecimal; for example, \x1B is escape
\\	The "\" character
\t	The tab character (\x09)
\r	The return character (\x0D)
\n	The new line character \x0A)

Note The %### decimal syntax for specifying binary octets has been replaced with the \x## hexadecimal syntax. Migrated definitions will be converted automatically.

```
Example 1:
#
# Note: script comments start with a # character
#
# Send a simple text command
#
Send=Hello There

Example 2:
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
```

```
Example 3:
#
# Send a binary escape (27) an x y and z and then a nak (21)
#
Send=\x1Bxyz\x15
```

Script Syntax: SimpleExpect Keyword

The SimpleExpect keyword lets you specify expected responses from your server. Responses can be binary (that is, nonprintable ASCII character) responses. If you know exactly (or even approximately) what to expect you can construct a simple expect response string to match against.

This keyword allows you some flexibility in accepting variable responses and choosing only the information you need. If you need additional flexibility you may want to consider using the regular expression syntax available in the Expect Keyword.

The SimpleExpect form is SimpleExpect=Response. Where the response is just a series of characters you expect back from the service. The following table displays keywords that match logic and wildcards to compare responses byte by byte expanding escape codes as you go.

Command Options

Keyword	Description
\x##	Binary value in hexadecimal; for example,\x00 is null
.	Matches any character
\%	The "%" character
\.	The "**.**" character
\\	The "\" character

Note Only the number of characters specified in the expect string are used to match the response. The response is expected to start with these characters. Any extra trailing characters received are just ignored.

```
Example 1:
#
# Note: script comments start with a # character
#
# Send=Hello There
#
# Expect a nice response
#
SimpleExpect=Hi, how are you?

Example 2:
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
#
# Expect a large response, be we only care to check that first word
# received is "Customer"
#
SimpleExpect=Customer

Example 3:
#
# Send a binary escape (27) an x y and z and then a nak (21)
#
Send=\x1B\x15
#
# Expect any byte (we don't care) then an abc and an ack (6)
#
SimpleExpect=.abc\x06
```

Send to Disconnect Examples

For a service such as FTP, the command would be **`QUIT/r/n`**. If a command string is not specified, the connection is closed by sending a FIN packet and then an RST packet.

The /r (carriage return) and /n (line feed) are the conventions for sending these control characters to terminate a string. You can use:

- /r = 0x0a
- /n = 0x0d
- /t = 0x09 or /xnn where nn is any hexadecimal value from 00 to FF

The disconnect string is:

Send=QUIT/r/n

Regular Expression Syntax

The following tables list the syntax understood by the Cisco netManager Regex Engine:

Table 8-1 Matching a Single Character

Meta-Character	Description	Matches
`.`	Dot	Matches any one character.
`[...]`	Character class	Matches any character inside the brackets. For example, [abc] matches a, b, and c.
`[^...]`	Negated character class	Matches any character except those inside the brackets. For example, [^abc] matches all characters except a, b, and c.
`-`	Dash	Used within a character class. Indicates a range of characters. For example: • [2-7] matches any of the digits 2 through 7. • [0-3a-d] is equivalent to [0123abcd].
`\`	Escaped character	Interpret the next character literally. For example, 3\.14 matches only 3.14, whereas 3.14 matches 3234, and so on

`\xnn`	Binary character	Match a single binary character. nn is a hexadecimal value between 00 and FF. For example: • \x41 matches A. • \x0B matches Vertical Tab.

Table 8-2 Quantifiers

Meta-Character	Description	Matches
?	Question	One optional. The preceding expression once or not at all. For example, colou?r matches colour or color. For example, [0-3][0-5]? matches 2 and 25.
*	Asterisk	Optional. Any number allowed. For example, .* Zero or more occurrences of any character.
+	Plus	One required, additional are optional. For example, [0-9]+ matches 1, 15, 220, and so on.
??, +?, *?		Nongreedy versions of ?, +, and *. Match as little as possible, whereas the greedy versions match as much as possible. For example, for input string <html>content</html>. <.*?> matches <html> <.*> matches <html>content</html>

Table 8-3 Matching Position

Meta-Character	Description	Matches
^	Caret	Matches the position at the start of the input. For example: • ^2 will only match input that begins with 2. • ^[45] will only match input that begins with 4 or 5.
$	Dollar	At the end of a regular expression, this character matches the end of the input. For example, >$ matches a right arrow symbol (>) at the end of the input.

Table 8-4 Other

Meta-Character	Description	Matches
|	Alternation	Matches either of the expressions that it separates. For example, H|Cat matches either Hat or Cat.
(...)	Parentheses	Provides grouping for quantifiers; limits scope of alternation via precedence. For example, (abc)* matches 0 or more occurrences of the the string abc.

`\0, \1, ...`	Backslash	Matches text previously matched within first, second (and so on) match group (starting at 0). For example, <{head}>.*?</\0> matches "<head>xxx</head>".
!	Negation	The expression following ! does not match the input. For example, a!b matches a not followed by b.

Table 8-5 Abbreviations

Abbreviation	Matches
\a	Any alphanumeric character: (A-Z, a-z, 0-9).
\b	White space (blank): ([\\t]).
\c	Any alphabetic character: ([a-zA-Z]).
\d	Any decimal digit: [0-9].
\D	Any nondecimal digit [^0-9].
\h	Any hexadecimal digit: ([0-9a-fA-F]).
\n	New line: (\r|(\r?\n)).
\p	Any punctuation character: ,./\';:"!?@#$%^&*()[]{}- _=+|<>!~.
\P	Any nonpunctuation character.
\q	A quoted string: (\"[^\"]*\")|(\'[^\']*\').
\s	Cisco netManager-style white space character [\\t\\n\\r\\f\\v].
\S	Cisco netManager-style nonwhite space character [^ \\t\\n\\r\\f\\v].
\w	Part-of-word character ([a-zA-Z0-9_]).
\W	nonword character ([^a-zA-Z0-9_]).
\z	An integer: ([0-9]+).

Text String Example

To check an Internet Relay Chat (IRC) service, you can send the command **Version/r/n;** and the expected response from the IRC service is irc.

```
Name: IRC; Port: 6667; TCP.
Send=Version/r/n
Expect=irc
Send=QUIT/r/n
```

Note You can use Telnet to find the proper value for **SimpleExpect**, or an **Expect** string for a particular service. Packet capture tools can also be very useful.

Using Telnet to Determine "Expect on Connect" String

Telnet to the desired port on the host when you are certain it is working properly, and see what comes back. You can enter just an identifying portion of a SimpleExpect or Expect keyword.

For example, if you expect to get "220 hostname.domain.com Imail v1.3" back from the host, you could use "220 host" as a response string (that is, `SimpleExpect=220 host`, or `Expect=^220 host`).

Note Some services are based on binary protocols (such as DNS) and will not provide you with a simple response string to use. You can use a packet capture tool to view these types of responses.

Using Active Script Monitor

The Active Script Monitors let you write either VBScript or JScript code to perform a check on a device. If the script returns an error code, the monitor is considered down.

Note Cisco netManager does not support the scripts that you create, only the ability to use them in the Active Script Monitor.

- **Name**. The name of the monitor as it appears in the Active Monitor Library.
- **Description**. The description of the monitor as it appears in the Active Monitor Library.
- **Timeout**. The amount of time (in seconds) Cisco netManager should wait for a response to the poll.

Note Though the maximum timeout is 60 seconds, you should not use a timeout longer than the default of 10 seconds. You should use the shortest timeout possible.

- **Script type**. VBScript or JScript
- **Script text**. Write or insert your monitor code here.
- **Use in discovery**. Select this option to have the monitor appear in the active monitor list during discovery. From there, you can select the monitor to have Cisco netManager discover that monitor type in your devices.

This script monitor has a context object that you can use to poll for specific information about the device.

Examples: Active Script Monitor Context Code

The following table lists several examples of active script monitor context code that you can use to create useful active monitors for your devices. To use these examples, select the text of the context and then copy and paste the code into the **Script text** box of the Active Script Monitor dialog box.

Note If the copyright information appears in the text that you copied and pasted from the filter, you should delete it.

Table 8-6 Context Code Examples

Monitor	Code

How to return the results of the script to Cisco netManager.
Note This affects the state of the device.
	JScript:
	`Context.SetResult(0, "    Everything is OK"); //Success`
	`Context.SetResult(1, "    Really big big error"); //Failure`
	VBScript:
	`Context.SetResult 1, "    Really big big error"`

Logging a message to the Cisco netManager event viewer. **Note** To view Context.LogMessage entries, you must have selected **Debug On** in the event viewer.	JScript: `Context.LogMessage("This is the message");`
Accessing the Device ID.	JScript: `var nDeviceID = Context.GetProperty("DeviceID");`
Accessing the IP address of the device.	JScript: `var sAddress = Context.GetProperty("Address");`

Accessing the device credentials.
Note All passwords are decrypted.
	JScript:
	`var sV1ReadCommunity = Context.GetProperty("CredSnmpV1:ReadCommunity");`
	`var sV1WriteCommunity = Context.GetProperty("CredSnmpV1:WriteCommunity");`
	`var sV2ReadCommunity = Context.GetProperty("CredSnmpV2:ReadCommunity");`
	`var sV2WriteCommunity = Context.GetProperty("CredSnmpV2:WriteCommunity");`
	`var sNTUsername = Context.GetProperty("CredWindows:DomainAndUserid");`
	`var sNTPassword =  Context.GetProperty("CredWindows:Password");`

<table>
<tr><th>Monitor</th><th>Code</th></tr>
<tr><td>Use WMI to see who is currently logged into a device.</td><td>

You can set the monitor to be down if the logged-in user is not the expected user.

```
VBScript:

sComputer = Context.GetProperty("Address")
nDeviceID = Context.GetProperty("DeviceID")

'Assuming ICMP is not blocked and there's a ping monitor on the device, we want to
'perform the actual check only if the Ping monitor is up. ConnectServer method of
'the SWbemLocator has a long time out so it would be good to avoid unnecessary tries.
'Please note: there's no particular polling order of active monitors on a device.
'During each polling cycle, it's possible that this monitor could be polled before
'Ping is polled. If the network connection just goes down but Ping is not polled yet,
'and therefore still has an up state, this active monitor will still do an actual
'check and experience a real down. But for the subsequent polls, it won't be doing a
'real check (ConnectServer won't be called) as Ping monitor has a down state, and this
'monitor will be assumed down.

If IsPingUp(nDeviceID) = false Then
Context.SetResult 1,"Actual check was not performed due to ping being down. Automatically set to down."
Else
sAdminName = Context.GetProperty("CredWindows:DomainAndUserid")
sAdminPasswd = Context.GetProperty("CredWindows:Password")

    sLoginUser = GetCurrentLoginUser(sComputer, sAdminName, sAdminPasswd)
sExpectedUser = "administrator"
If Not IsNull(sLoginUser) Then
If instr(1,sLoginUser, sExpectedUser,1) > 0  Then
Context.SetResult 0,"Current login user is " & sLoginUser
ElseIf sLoginUser = " " Then
  Context.SetResult 0,"No one is currently logged in."
Else
  Context.SetResult 1,"an unexpected user " & sLoginUser & " has logged in " & sComputer
End If
End If
End If
'Check if Ping monitor on the device specified by nDeviceID is up.
'If nDeviceID is not available as it's in the case during discovery, then assume
'ping is up.
'If ping monitor is not on the device, then assume it's up so the real check will be
'performed.
```

</td></tr>
</table>

<table>
<tr><th>Monitor</th><th>Code</th></tr>
<tr><td>Use WMI to see who is currently logged into a device.
(continued)</td><td>

```
Function IsPingUp(nDeviceID)
If nDeviceID > -1 Then
'get the Ping monitor up state.
sSqlGetUpState = "SELECT sStateName from PivotActiveMonitorTypeToDevice as P
join " & _
"ActiveMonitorType as A on P.nActiveMonitorTypeID=A.nActiveMonitorTypeID " &
_
"join MonitorState as M on P.nMonitorStateID = M.nMonitorStateID " & _
"where nDeviceID=" & nDeviceID & " and A.sMonitorTypeName='Ping' and " & _
                      " P.bRemoved=0"
Set oDBconn = Context.GetDB
Set oStateRS = CreateObject("ADODB.Recordset")
' oStateRS.ActiveConnection = oDBconn
' oStateRS.CursorType =3  'adOpenStatic cursorType
       oStateRS.Open sSqlGetUpState,oDBconn,3
'if recordset is empty then
If oStateRS.RecordCount = 1 Then
If instr(1,oStateRS("sStateName"),"up",1) > 0 Then
IsPingUp = true
  Else
     IsPingUP = false
  End If
Else
  'if there's no ping on the device, then just assume up, so regular check
will happen.
  IsPingUp= true
End If
oStateRS.Close
oDBconn.Close
Set oStateRS = Nothing
Set oDBconn = Nothing
Else
'assume up, since there's no device yet. It's for scanning during discovery.
 IsPingUP = true
End If
End Function
'Try to get the current login user name.
Function GetCurrentLoginUser(sComputer, sAdminName, sAdminPasswd)
GetCurrentLoginUser=Null
Set oSWbemLocator = CreateObject("WbemScripting.SWbemLocator")
On Error Resume Next
Set oSWbemServices = oSWbemLocator.ConnectServer _
  (sComputer, "root\cimv2",sAdminName,sAdminPasswd)
If Err.Number <> 0 Then
 Context.LogMessage("The 1st try to connect to " & sComputer & " failed. Err:"
& Err.Description)
 Err.Clear
      'If the specified user name and password for WMI connection failed, then
 'try to connect without user name and password. Can't specify user name
 'and password when connecting to local machine.
On Error Resume Next
 Set oSWbemServices = oSWbemLocator.ConnectServer(sComputer, "root\cimv2")
 If Err.Number <> 0 Then
    Err.Clear
```

</td></tr>
</table>

Monitor	Code
Use WMI to see who is currently logged into a device. (continued)	On Error Resume Next Context.SetResult 1,"Failed to access " & sComputer & " " & _ "using username:" & sAdminName & " password." & " Err: " & Err.Description Exit Function End If End If Set colSWbemObjectSet = oSWbemServices.InstancesOf("Win32_ComputerSystem") For Each oSWbemObject In colSWbemObjectSet On Error Resume Next 'Context.SetResult 0,"User Name: " & oSWbemObject.UserName & " at " & sComputer sCurrentLoginUser = oSWbemObject.UserName Err.Clear Next If Cstr(sCurrentLoginUser) ="" Then GetCurrentLoginUser = " " Else GetCurrentLoginUser = sCurrentLoginUser End If Set oSWbemServices = Nothing Set oSWbemLocator = Nothing End Function

Use SNMP to monitor the total bandwidth utilization on an interface (in + out octets) by polling values of the interface MIB.	JScript:
	// Settings for this monitor:
	// the interface index ifIndex:
	var nInterfaceIndex = 65540;
	// this monitor will fail if the interface utilization goes above this current ratio:
	// current bandwidth / maxBandwidth > nMaxInterfaceUtilizationRatio
	var nMaxInterfaceUtilizationRatio = 0.7; // Set to 70%
	// Create an SNMP object, that will poll the device.
	var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
	// Get the device ID
	var nDeviceID = Context.GetProperty("DeviceID");
	// This function polls the device returns the ifSpeed of the inteface indexed by nIfIndex.
	// ifSpeed is in bits per second.
	function getIfSpeed(nIfIndex)
	{

Monitor	Code

Use SNMP to monitor the total bandwidth utilization on an interface (in + out octets) by polling values of the interface MIB.
(continued)
	`var oResult = oSnmpRqst.Initialize(nDeviceID);`
	`if(oResult.Failed)`
	`{`
	`    return null;`
	`}`
	`return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.5." + nIfIndex)); // ifSpeed`
	`}`
	`// Function to get SNMP ifInOctets for the interface indexed by nIfIndex (in bytes).`
	`// Returns the value polled upon success, null in case of failure.`
	`function getInOctets(nIfIndex)`
	`{`
	`var oResult = oSnmpRqst.Initialize(nDeviceID);`
	`if(oResult.Failed)`
	`{`
	`    return null;`
	`}`
	`return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.10." + nIfIndex)); // inOctets`
	`}`
	`// Function to get SNMP ifOutOctets for the interface indexed by nIfIndex (in bytes).`
	`// Returns the value polled upon success, null in case of failure.`
	`function getOutOctets(nIfIndex)`
	`{`
	`var oResult = oSnmpRqst.Initialize(nDeviceID);`
	`if(oResult.Failed)`
	`{`
	`   return null;`
	`}`
	`return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.16." + nIfIndex)); //  outOctets`
	`}`
	`// Helper function to get a specific SNMP object (OID in sOid).`
	`// Returns the value polled upon success, null in case of failure.`
	`function SnmpGet(sOid)`
	`{`
	`var oResult = oSnmpRqst.Get(sOid);`
	`if(oResult.Failed)`
	`{`
	`   return null;`
	`}`
	`else`
	`{`
	`return oResult.GetPayload;`
	`}`
	`}`
	`// Get the current date. It will be used as a reference date for the SNMP polls.`
	`var oDate = new Date();`
	`var nPollDate = parseInt(oDate.getTime()); // get the date in millisec in an integer.`
	`// Do the actual polling:`
	`var nInOctets = getInOctets(nInterfaceIndex);`

Monitor	Code

Use SNMP to monitor the total bandwidth utilization on an interface (in + out octets) by polling values of the interface MIB.
(continued)
	var nOutOctets = getOutOctets(nInterfaceIndex);
	var nIfSpeed = getIfSpeed(nInterfaceIndex);
	if (nInOctets == null || nOutOctets == null || nIfSpeed == null)
	{
	Context.SetResult(1, "Failure to poll this device.");
	}
	else
	{
	var nTotalOctets = nInOctets + nOutOctets;
	// Retrieve the octets value and date of the last poll saved in a context variable:
	var nInOutOctetsMonitorPreviousPolledValue =
	Context.GetProperty("nInOutOctetsMonitorPreviousPolledValue");
	var nInOutOctetsMonitorPreviousPollDate =
	Context.GetProperty("nInOutOctetsMonitorPreviousPollDate");
	if (nInOutOctetsMonitorPreviousPolledValue == null ||
	nInOutOctetsMonitorPreviousPollDate
	== null)
	{
	    // the context variable has never been set, this is the first time we are polling.
	    Context.LogMessage("This monitor requires two polls.");
	    Context.SetResult(0, "success");
	}
	else
	{
	// compute the bandwidth that was used between this poll and the previous poll
	var nIntervalSec = (nPollDate - nInOutOctetsMonitorPreviousPollDate)/1000;
	// time since
	    last poll in seconds
	var nCurrentBps = (nTotalOctets - nInOutOctetsMonitorPreviousPolledValue) *
	8 /
	nIntervalSec;
	Context.LogMessage("total octets for interface " + nInterfaceIndex + " = "
	+ nTotalOctets)
	;
	Context.LogMessage("previous value = " +
	nInOutOctetsMonitorPreviousPolledValue);
	Context.LogMessage("difference: " + (nTotalOctets -
	nInOutOctetsMonitorPreviousPolledValue)
	+ " bytes");
	Context.LogMessage("Interface Speed: " + nIfSpeed + "bps");
	Context.LogMessage("time elapsed since last poll: " + nIntervalSec + "s");
	Context.LogMessage("Current Bandwidth utilization: "+ nCurrentBps + "bps");
	if (nCurrentBps/nIfSpeed > nMaxInterfaceUtilizationRatio)
	{
	   Context.SetResult(1, "Failure: bandwidth used on this interface " +
	nCurrentBps + "bps
	   / total available: " + nIfSpeed + "bps is above the specified ratio: " +
	
	   nMaxInterfaceUtilizationRatio);
	   }

Monitor	Code

Use SNMP to monitor the total bandwidth utilization on an interface (in + out octets) by polling values of the interface MIB.
(continued)
	else
	{
	Context.SetResult(0, "Success");
	}
	}
	// Save this poll information in the context variables:
	Context.PutProperty("nInOutOctetsMonitorPreviousPolledValue", nTotalOctets)
	Context.PutProperty("nInOutOctetsMonitorPreviousPollDate", nPollDate);
	}

Monitoring an SNMP agent running on a nonstandard port (161).	JScript:
	var nSNMPPort = 1234; // change this value to the port your agent is running on
	var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
	// Get the device ID
	var nDeviceID = Context.GetProperty("DeviceID");
	// Initialize the SNMP request object
	var oResult = oSnmpRqst.Initialize(nDeviceID);
	if(oResult.Failed)
	{
	Context.SetResult(1, oResult.GetPayload);
	}
	else
	{
	// Set the request destination port.
	var oResult = oSnmpRqst.SetPort(nSNMPPort);
	// Get sysDescr.
	var oResult = oSnmpRqst.Get("1.3.6.1.2.1.1.1.0");
	if (oResult.Failed)
	{
	Context.SetResult(1, "Failed to poll device using port " + nSNMPPort + ". Error=" +
	oResult.GetPayload);
	}
	else
	{
	Context.SetResult(0, "SUCCESS. Detected an SNMP agent running on port " + nSNMPPort);
	}
	}

Using the Active Script Monitor Context Object

The context object is available to the script programmer when scripts are executing. It delivers context aspects of the device that it is operating upon. All methods and properties are retrieved using the "Context" namespace.

We have provided several code samples for you to use to create active script monitors for your devices.

Methods	Code

LogMessage(sText);	Allows for a message to be written to the Cisco netManager debug log.
	For example,
	JScript:
	`Context.LogMessage( "Checking Monitor name using Context.GetProperty()");`
	VBScript:
	`Context.LogMessage "Checking Address using Context.GetProperty()"`

PutProperty(sPropertyName);	Allows you to store a value in the INMSerialize object. This value is retained across polls.
	For example,
	JScript:
	`var nCount = parselnt(nNum) +1;`
	`Context.PutProperty("MyNumeric",nCount);`

SetResult(nCode, sText);	Allows for a result code and result message to be set. This is how you can tell the Cisco netManager system if the monitor succeeded or not.
	Note Every script should have a result, otherwise it will report back positively.
	For example,
	JScript:
	`Context.SetResult(0, "    Everything is OK"); //Success`
	`Context.SetResult(1, "    Really big big error"); //Failure`
	VBScript:
	`Context.SetResult 1, "    Really big big error"`

Properties

```
GetProperty(sPropertyName);
```

This property offers access to many device-specific aspects. You obtain access to these items using the names listed. These names are case sensitive.

Names	Description
ActiveMonitorTypeName	The active monitor display name
Address	The IP address of the device
DeviceID	The device ID
Mode	1 = Doing discovery 2 = Polling 3 = Test
ActiveMonitorTypeID	The active monitor's type ID
CredSnmpV1:ReadCommunity	SNMPv1 read community
CredSnmpV1:WriteCommunity	SNMPv1 write community
CredSnmpV2:ReadCommunity	SNMPv2 read community
CredSnmpV2:WriteCommunity	SNMPv2 write community
CredWindows:DomainAndUserid	Windows NT domain and user ID
CredWindows:Password	Windows NT password

Properties Example1 1

JScript:

```
var sAddress = Context.GetProperty("Address");
var sReadCommunity = Context.GetProperty("CredSnmpV1:ReadCommunity");
var nDeviceID = Context.GetProperty("DeviceID");
```

JScript:

```
//Sending log message to the Cisco netManager Event Viewer
Context.LogMessage ( "Checking Mode flag");
var nFlag = Context.GetProperty("Mode");

if (nFlag == 1)
{
Context.LogMessage ("Doing a discovery");
}
else if (nFlag == 2)
{
Context.LogMessage ("Doing a poll");
}
else if (nFlag == 3)
{
```

```
Context.LogMessage ("Must be just a test.");
}
else
{
Context.LogMessage ("Do not know the mode.");
}
//Set the result code of the check (0=Success, 1=Error)
Context.SetResult (0, "No error");
(GetDB);
```

This property returns an open connection to the Cisco netManager database.

Properties Example 2

This example gets the Open connection and reads some values out of the Cisco netManager "Device" table using the deviceID context.

```
var oDb = Context.GetDB;
if (null == oDb)
{
Context.SetResult( 1, "  Problem creating the PRO DB object");
}
else
{
var oRs = new ActiveXObject("ADODB.Recordset");
// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");
var sSql = "SELECT * from Device WHERE nDeviceID = " + nDeviceID;
oRs = oDb.Execute(sSql);
if ( !oRs.EOF )
{
   var sDisplay;
   sDisplay = "" + oRs("sDisplayName");
   Context.LogMessage("Display Name=" + sDisplay);
   sDisplay = "" + oRs("nWorstStateID");
   Context.LogMessage("WorstStateID=" + sDisplay);
   sDisplay = "" + oRs("sNote");
   Context.LogMessage("Note=" + sDisplay);
   sDisplay = "" + oRs("sStatus");
   Context.LogMessage("Status=" + sDisplay);
}
Context.SetResult( 0, "   Ok");
}
```

CHAPTER 9

Using Passive Monitors

Unlike active monitors or performance monitors, which actively poll a device to check its status or to gather statistical data, passive monitors passively listen for events on devices.

Because it does not repeatedly poll devices and wait for a device to signal a problem, a passive monitor uses fewer resources than an active monitor both on the machine running Cisco netManager and on the network.

Passive monitors are also useful because some devices on a network may not provide a clear up or down status when queried. For example, a message may get logged to the system's Event log by another application (such as an antivirus application alerting when a virus is found). Since these messages or events can occur at any time, a Passive Monitor Listener listens for them, and notifies Cisco netManager when they occur.

However, the information that can be reported in a passive monitor event is not as customizable as it is with active monitors. In the case of a severe device failure, a device may enter a state where it is not able to successfully send a passive monitor event. A connectivity loss may prevent the Cisco netManager system from receiving an event sent to it as well.

Passive monitors should be used to complement active monitors, but you should not rely solely on passive monitors to monitor a device or service.

The first step in using this function is to configure the Passive Monitor Listeners. For more information, see Configuring Passive Monitor Listeners, page 9-1. After the listeners have been configured, you can Configure passive monitors for individual devices. For more information, see Adding or Editing Passive Monitors, page 9-2.

Passive Monitors Icon

When a passive monitor is configured on a device, the device icon displays a diamond shape on the upper left side. This shape changes color when an unacknowledged state change occurs on the monitor. After the device has been acknowledged, the icon returns to the previous color.

Configuring Passive Monitor Listeners

A Passive Monitor Listener listens for an event to occur and then notifies Cisco netManager. This lets you get notification of an event when it occurs, rather than requiring you to poll for all event types. The Passive Monitor Listener is solely responsible for how it monitors its events. This means that the server could listen for network traffic or application-specific events.

Cisco netManager is installed with three Passive Monitor Listeners:

- **SNMP Passive Monitor (SNMP Trap)**—A trap is an unsolicited SNMP message sent from a device to indicate a change in status, such as a router indicating one of its interfaces went down or a printer indicating that it is out of paper.
- **Syslog Passive Monitor**—A syslog monitor 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 could contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.
- **Windows Event Log Monitor**—This could be monitoring when a service is started or stopped, if there was a logon failure recorded, or any other entry in the Windows Event log

Using the Passive Monitor Library

The Passive Monitor Library dialog displays the passive monitor types that have been created for Cisco netManager. These types are specific configurations of SNMP traps, Windows Log Events, and Syslog Events. After the Monitor types have been configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog.

Step 1 From the Cisco netManager web interface, click **GO > Configure > Passive Monitor Library**.

or

From the main menu bar of the Cisco netManager console, click **Configure > Passive Monitor Library**.

Step 2 Click **New** to create a new passive monitor type.

Step 3 Select a monitor type in the list, then click **Edit** to change the settings.

Step 4 Select a monitor type in the list, then click **Copy** to create a new monitor type based on the selected type.

Step 5 Select a monitor type, then click **Delete** to remove it from the list.

Adding or Editing Passive Monitors

To add/edit a passive monitor:

Step 1 From the Cisco netManager web interface, click **GO > Configure > Passive Monitor Library**.

Step 2 Do one of the following:

- Click **New** to configure a new passive monitor.
- Select a monitor from the list, then click **Edit** to make changes to an existing configuration. The configuration dialog for the selected monitor type opens.

Step 3 After you make the necessary changes, click **OK** to add the monitor to the list or to save the changes you made to a monitor already on the list.

Assigning a Passive Monitor to a Device

Step 1 Right-click the device to which you want to assign a passive monitor, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Passive Monitors**. The Device Properties Passive Monitor dialog opens.

Step 3 Click **Add**. The Passive Monitor Properties dialog opens.

Step 4 Select the passive monitor type and passive monitor you want to assign, then click **Next**. The Setup Actions for Passive Monitors dialog opens.

Step 5 Click **Add** to set up a new action for the passive monitor. The Select or Create Action dialog opens. Click one of the following:

- Select an action from the Action Library
- Create a new action

Step 6 Click **Finish** to add the passive monitor to the device.

Accessing Group and Device Passive Monitor Reports

The following reports display information for devices or device groups that have passive monitors configured and enabled. Access these reports from the web interface Reports tab. For more information, see Chapter 11, “Using Reports.”

- SNMP Trap log
- Syslog Entries
- Windows Event log
- Passive Monitor Error log

Receiving SNMP Traps

Cisco netManager has an internal SNMP trap handler, which, when enabled, listens for and accepts SNMP traps that are addressed to it. Cisco netManager records the trap in the device's SNMP Trap log.

You can also set up Cisco netManager to fire an action when a trap is received for a device.For more information, see Using the Trap Definition Import Tool, page 12-4.

To configure Cisco netManager to receive traps:

Step 1 On the devices that will be monitored, set the SNMP agent to send traps to Cisco netManager. Trap manager addresses must be set on each physical device. This cannot be done from Cisco netManager.

Step 2 Set up the MIB entries for traps by placing the MIB text file in the `Mibs` directory.

Step 3 Enable the SNMP Trap Handler

a. From the Cisco netManager console, select **Configure** > **Program Options**.

b. Select **Passive Monitor Listeners**.

c. Select **SNMP Trap**.

d. Click the **Configure** button.

e. Select the appropriate options:

- **Listen for messages on port**. Select this option if you want Cisco netManager to listen for SNMP traps. The standard SNMP trap port is 162, but you can change this port to a nonstandard number. The changes are immediate, and you do not have to restart Cisco netManager for the changes to be in effect.
- **Accept unsolicited SNMP traps**. If this is not selected, *only* traps which are specifically added to devices as events are logged to the activity log and are able to trigger alerts. You may prefer to select this option so that *all* traps which occur can be detected and logged to the activity log. Note that regardless of this filter setting, traps are logged to the SNMP Trap log. By default there is no strict filtering of traps; this way you can see all traps from all sources, then make decisions about creating Actions based on specific traps you have seen. Later you may make the decision to filter out all traps except those you expect to see.
- **Forward traps**. Select this option to forward traps to IP addresses added to the **Forward traps to** list.
- **Forward unsolicited traps**. Select this option to forward all traps, including unsolicited traps.
- **Forward traps to**. Click **Add** to add an IP address and port to forward traps to. You can forward traps to multiple IP addresses.

f. Click **OK** to save changes.

Note Installing the SNMP agent on the Cisco netManager machine also starts an SNMP trap service. This can result in a port conflict, because both the SNMP trap service and the Cisco netManager SNMP trap handler listen on port 162. To eliminate this problem, you need to disable the SNMP trap service.

CHAPTER 10

Using Performance Monitors

Performance Monitors in Cisco netManager gather important information about the devices running on your network, then use that data to create reports trending the utilization and availability of different aspects of those devices.

Through Cisco netManager, you can gather statistics on the following:

- CPU Utilization
- Disk Utilization
- Interface Utilization
- Memory Utilization
- Ping Latency and Availability
- Temperature Statistics
- Cisco Unity Port Utilization

Through Cisco netManager, you can gather status on the following:

- Cisco Unified Communications Manager Logical Connectivity
- Cisco Unified Communications Manager Express Logical Connectivity
- Cisco Unified Communications Manager Express Status
- Cisco Unity Status
- Cisco Unity Express Status
- Device Inventory Entity Status
- Fan Status
- Power Supply Status
- SRST Status
- Voice Services Status
- Wireless LAN Controller

Note These performance monitors in the library cannot be edited or removed.

The system also lets you create custom performance monitors that you can use to monitor any performance counter made available through WMI or SNMP, as well as the use of JScript and VBScript.

Performance monitors are configured in the Performance Monitor Library, and added to individual devices through **Device Properties > Performance Monitors**. You can create global WMI, SNMP, and active script monitors in the library, or create device-specific monitors in Device Properties.

Understanding the Performance Monitor Library

The Performance Monitor Library is a central storehouse of all global Performance Monitors that have been configured for your network. Performance monitors gather information about specific WMI and SNMP values from the network devices.

You can use the Performance Monitor Library to configure and manage performance monitors. When custom Performance Monitors are changed, the changes affect each instance of that particular monitor across your device groups. To access the Performance Monitor Library dialog box, do one of the following:

- From the Cisco netManager console main menu, select **Configure** > **Performance Monitor Library**.
- From the Cisco netManager web interface, select **GO > Configure > Performance Monitor Library**.

To configure Performance Monitors for the devices they are assigned to:

Step 1 Right-click a device you want to configure. The shortcut menu opens.

Step 2 Click **Properties**. The Device Properties dialog box opens.

Step 3 Click **New** to configure a new monitor.

Step 4 Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.

Step 5 Select a performance monitor type, then click **Delete** to remove it from the list.

Step 6 Click **OK** to save changes.

Enabling SNMP on Windows Devices

Before you can collect performance data on a Windows PC, you must first install and enable the Microsoft SNMP Agent on the device itself.

To install SNMP Monitoring:

Step 1 From the Windows Control Panel, click **Add or Remove Programs**.

Step 2 Click **Add/Remove Windows Components**.

Step 3 From the Components list, select **Management and Monitoring Tools**.

Step 4 Click **Details** to view the list of subcomponents.

Step 5 Make sure Simple Network Management Protocol is selected.

Step 6 Click **OK**.

Step 7 Click **Next** to install the components.

Step 8 After the installation wizard is complete, click **Finish** to close the window.

To enable SNMP monitoring:

Step 1 In the Control Panel, click **Administrative Tools**.

Step 2 Double-click **Services**. The Services console opens.

Step 3 In the Services (Local) list, double-click **SNMP Service** to view the properties.

Step 4 On the **Agent** tab, enter the contact name for the person responsible for the upkeep and administration of the computer, then enter the location of the computer. These items are returned during some SNMP queries.

Step 5 On the **Security** tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like Cisco netManager to read information about the computer. This community string will be used later to create credentials for connecting to this device.

Step 6 On the **General** tab, click **Start** to start the service (if necessary).

Step 7 Click **OK** to close the dialog box.

Configuring and Enabling Performance Monitors

Cisco netManager is installed with many performance monitors that monitor specific types of data on your devices. These monitors appear in the Performance Monitor Library.

If you select a specific performance monitor without configuring the monitor manually, the default collection type is automatically selected. The collection type refers to the item on the current device that is being monitored (This does not pertain to the custom WMI and SNMP monitors that may appear). For Cisco devices all performance monitors, except Interface Utilization and Ping Latency and Availability, will be enabled by default.

Performance monitors are associated with the device based on its capabilities:

Capability	Performance Monitor
Autonomous Access Point	CPU Utilization
	Memory Utilization
	Interface Status
Cisco ASA	Device Inventory Entity Status
	CPU Utilization
	Memory Utilization
	Interface Status
Cisco Unified Communications Manager	Communications Manager Status
	Communications Manager Logical Connectivity
	Device Inventory Entity Status

Capability	Performance Monitor
Cisco Unified Communications Manager Express	Communications Manager Express Status
	Communications Manager Express Logical Connectivity
	Device Inventory Entity Status
Cisco Unity	Unity Status
	Unity Port utilization
	Device Inventory Entity Status
Cisco Unity Connection	Unity Status
	Unity Port Utilization
	Device Inventory Entity Status
Cisco Unity Express	Unity Express Status
	Interface Status
	Device Inventory Entity Status
Cisco PIX Firewall	Device Inventory Entity Status
	CPU Utilization
	Memory Utilization
	Interface Status
Cisco IDS	CPU Utilization
	Memory Utilization
	Interface Status
Cisco IPS	CPU Utilization
	Memory Utilization
	Interface Status
MCS	CPU Utilization
	Memory Utilization
	Disk Utilization
	Temperature Statistics
	Power Supply Status
	Fan Status
	Voice Services Status
	Interface Status
	Device Inventory Entity Status
MPX	Voice Services Status
	Memory Utilization
	Disk Utilization
	CPU Utilization
	Interface Status
	Device Inventory Entity Status

Capability	Performance Monitor
Router	CPU Utilization
	Memory Utilization
	Temperature Statistics
	Interface Status
	Power Supply Status
	Fan Status
	Device Inventory Entity Status
SRST	SRST Status
	Device Inventory Entity Status
Switch	CPU Utilization
	Memory Utilization
	Temperature Statistics
	Interface Status
	Power Supply Status
	Fan Status
	Device Inventory Entity Status
Cisco VPN	Interface Status
Wireless LAN Controller	Wireless LAN Controller Status
	Interface Status
	CPU Utilization
	Memory Utilization

For all other devices, the following performance monitors are associated:

- CPU Utilization
- Memory Utilization
- Disk Utilization
- Interface Utilization
- Ping Latency and Availability

To configure monitors for use on specific devices, you must use either the **Device Properties > Performance Monitors** to configure for a single device, or **Bulk Field Change > Performance Monitors** to configure for multiple devices.

To enable a global performance monitor for a single device:

Step 1 On the Device tab, select a device from the device list.

Step 2 Right-click and choose **Properties** from the right-click menu to view the device properties.

Step 3 Click **Performance Monitors** to view the Performance Monitors dialog box.

Step 4 From the top section of the dialog box, select the global performance monitor you would like to enable for the selected device.

Note To enable a CPU, disk, interface, or memory global performance monitor, you must first select and SNMP credential for the device from the SNMP credential page.

Step 5 Click **OK** to save the changes.

To configure a global performance monitor for a single device:

Step 1 On the Device tab, select a device from the device list.

Step 2 Right-click and choose **Properties** from the right-click menu to view the device properties.

Step 3 Click **Performance Monitors** to view the Performance Monitors dialog box.

Step 4 In the top section of the dialog box, select a global performance monitor, then click **Configure**.

Step 5 On the monitor configuration dialog box, select the specific item you want to monitor by making a selection in the **Collect data for** drop-down list. Depending on the monitor, you can select to collect data for **All**, **Active**, **Specific**, or **Default** interfaces, memories, CPUs, or disks.

If you select **Specific**, the list is enabled and you can select or clear the selection for any of the items in the list. This is particularly useful with the Interface Utilization monitor where a device may have many interfaces.

Step 6 Select the **Data collection interval**. This is the amount of time between performance polls.

Step 7 Click **Advanced** to change connection settings on the device.

Step 8 Click **OK** to save the changes.

Note To enable a global performance monitor for multiple devices, use the Bulk Field Change feature for performance monitors.

For information on the Active Script Performance Monitor, see Chapter 10, "Adding Custom Performance Monitors to the Performance Monitor Library."

Adding Custom Performance Monitors to the Performance Monitor Library

Performance monitors gather specific types of data on the devices they are assigned to. System-wide monitors are configured using the Performance Monitor Library, but you can also create specific SNMP and WMI monitors to be used on a per-device basis. The default performance monitors cannot be edited or changed from their default settings. By creating custom performance monitors, you can adjust the settings to fit your specific monitoring needs.

To create custom performance monitors (for system-wide use):

Step 1 In the Cisco netManager web interface, select **GO** > **Configure** > **Performance Monitor Library**.

Step 2 In the Performance Monitor Library, click **New.**

Step 3 Select the monitor type: SNMP, WMI, or Active Script Performance Monitor.

Step 4 Follow the instructions for the monitor type you have chosen as described in these topics:

- Configuring an SNMP Monitor, page 10-7
- Configuring an SNMP Active Script Performance Monitor, page 10-8

Configuring an SNMP Monitor

Step 1 In the Add SNMP Performance Counter dialog box, enter a name and a description for the monitor as it will appear in the Performance Monitor Library.

Step 2 Either enter the OID and instance or click the **Browse (...)** button next to the Instance box to go to the SNMP MIB Walker dialog box.

Step 3 In the MIB Walker dialog box, enter the share name or IP address of the computer to which you want to connect.

Step 4 Enter the SNMP credential used to connect to the device (or click the **Browse (...)** button to access the Credentials Library to create a new credential.)

Step 5 If needed, adjust the timeout and retry counts for the connection to the device.

Step 6 Click **OK.** The SNMP MIB Walker appears.

Step 7 Use the navigation tree in the left pane to select the specific MIB you want to monitor.

Step 8 In the right pane, select the Property of the MIB you want to monitor. You can view more information about the property/value pair at the bottom of the dialog box.

Step 9 Click **OK** to add the OID to the Performance counter and Instance boxes in the Add SNMP Performance counter dialog box.

Step 10 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.

Configuring a WMI Monitor

Step 1 On the Add WMI Performance Counter dialog, enter a name and description for the monitor, as it will appear in the Performance Monitor Library.

Step 2 Click the **Browse (...)** button next to the Instance box.

Step 3 In the dialog that appears, enter the share name or IP address of the computer in which you want to connect.

Step 4 Enter the domain and user login for the account on this computer. If a domain account is used, then the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user.

Step 5 Enter the password for the login used in the previous step and click **OK** to connect to the computer.

Step 6 Use the Performance counter tree to navigate to the performance counter you want to monitor.

Step 7 Once you select the performance counter, select the specific instance you want to monitor.

Step 8 Click **OK** to add the counter and instance to the Add Performance Counter dialog.

Step 9 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.

Note After the monitor has been added to the library, you can enable the monitor through **Device Properties** > **Performance Monitors** for that device.

Configuring an SNMP Active Script Performance Monitor

Step 1 On the Add Active Script Performance Monitor dialog box, enter a name and a description for the monitor as it will appear in the Performance Monitor Library.

Step 2 Enter a number for the timeout (in seconds).

Step 3 Choose the type of script (JScript or VBScript) you will be using to write the monitor from the Script type drop-down list.

Step 4 Add a new variable to the Reference Variables list by clicking **Add**.

Note You can add up to 10 reference variables to the monitor.

Step 5 On the Add reference variables dialog box, enter a name and description for the variable.

Step 6 Select the type of object (SNMP or WMI) from the 0bject type drop-down menu.

Step 7 If needed, adjust the timeout and retry counts for connection to the device.

Step 8 Click the **Browse (...)** button next to the Instance box. The SNMP MIB Browser appears.

Step 9 Enter the share name or IP address of the computer in which you are trying to connect.

Step 10 Enter the SNMP credential used to connect to the device (or click the **Browse (...)** button to access the Credentials Library to create a new credential.)

Step 11 If needed, adjust the timeout and retry counts for the computer in which you are trying to connect.

Step 12 Click **OK**. The SNMP MIB Walker appears.

Step 13 Use the navigation tree in the left panel to select the specific MIB you want to monitor. You can view more information about the property/value at the bottom of the dialog box.

Step 14 Click **OK** to add the OID to the Performance counter and Instance boxes in the Add new reference variable dialog box.

Step 15 Verify the configuration and click **OK** to add the variable to the Reference variable list on the Add Active Script Performance Monitor dialog box.

Step 16 Type or paste your monitor code in the Script text box.

Step 17 Click **OK** to save changes and add the monitor to the Performance Monitor Library.

Configuring a WMI Active Script Performance Monitor

Step 1 On the Add Active Script Performance Monitor dialog, enter a name and description for the monitor as it will appear in the Performance Monitor Library.

Step 2 Enter a number for the timeout (in seconds).

Step 3 Choose the type of script (JScript or VBScript) you will be using to write the monitor from the **Script type** drop down menu.

Step 4 Add a new variable to the Reference Variables list by clicking **Add**.

Note You can add up to 10 reference variables to the monitor.

Step 5 In the Add reference variables dialog, enter a name and description for the variable.

Step 6 Select the type of object (SNMP or WMI) from the Object type drop-down menu.

Step 7 Click the **Browse (...)** button next to the Instance box.

Step 8 In the dialog that appears, enter the share name or IP address of the computer in which you want to connect.

Step 9 Enter the domain and user login for the account on this computer. If a domain account is used, then the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user.

Step 10 Enter a password for the login used above and click **OK** to connect to the computer.

Step 11 Use the Performance counter tree to navigate to the performance counter you want to monitor.

Step 12 Once you select the performance counter, select the specific instance you want to monitor.

Step 13 Click **OK** to add the variable to the Reference variable list on the Add active script performance monitor dialog.

Step 14 Type your monitor code in the Script text box.

Step 15 Click **OK** to save changes and to add the monitor to the Performance Monitor Library.

Performance Reporting

After you have configured a performance monitor, you can generate a performance report to see the results of the performance polling attempts. A report can be used to troubleshoot your network problems.

The Reports tab contains all of the Cisco netManager full reports. You can use the Reports Overview page and the Reports Category drop-down list to navigate to reports according to their type and category.

All reports can be printed and many can also be exported into Microsoft Excel. A report can also be saved as an .html file for later review.

For more information on the Cisco netManager reports, see Chapter 11, “Using Reports.”

Performance monitors gather specific types of data on the devices they are assigned to. System-wide monitors are configured using the Performance Monitor Library, but you can also create specific SNMP and WMI monitors to be used on a per-device basis.

To configure an SNMP monitor:

Step 1 In the web interface, go to **GO** > **Configure** > **Performance** > **Monitor Library**.

Step 2 In the Performance Monitor Library, click **New**.

Step 3 Select **SNMP** as the monitor type.

Step 4 In the Add SNMP Performance Counter dialog box, enter a name and a description for the monitor as it will appear in the Performance Monitor Library.

Step 5 Either enter the OID and instance or click the **Browse (...)** button next to the Instance box to go to the SNMP MIB Walker dialog box.

Step 6 In the MIB Walker dialog, enter the share name or IP address of the computer to which you want to connect.

Step 7 Enter the SNMP credential used to connect to the device (or click the **Browse (...)** button to access the Credentials Library to create a new credential.)

Step 8 If needed, adjust the timeout and retry counts for the connection to the device.

Step 9 Click OK. The SNMP MIB Walker appears.

Step 10 Use the navigation tree in the left pane to select the specific MIB you want to monitor.

Step 11 In the right pane, select the property of that MIB you want to monitor. You can view more information about the property/value pair at the bottom of the dialog box.

Step 12 Click **OK** to add the OID to the Performance counter and Instance boxes in the Add SNMP Performance counter dialog box.

Step 13 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.

To configure a WMI monitor:

Step 1 In the web interface, go to **GO** > **Configure** > **Performance** > **Monitor Library**.

Step 2 In the Performance Monitor Library, click **New**.

Step 3 Select **WMI** as the monitor type.

Step 4 In the Add WMI Performance Counter dialog box, enter a name and a description for the monitor, as it will appear in the Performance Monitor Library.

Step 5 Click the **Browse (...)** button next to the Instance box.

Step 6 In the dialog box that appears, enter the share name or IP address of the computer to which you want to connect.

Step 7 Enter the domain and user login for the account on this computer. If a domain account is used, then the expected username is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user.

Step 8 Enter the password for the login used above and click **OK** to connect to the computer.

Step 9 Use the performance counter tree to navigate to the performance counter you want to monitor.

Step 10 Once you select the performance counter, select the specific instance you want to monitor.

Step 11 Click **OK** to add the counter and instance to the Add Performance Counter dialog box.

Step 12 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.

Note After the monitor has been added to the library, you can enable the monitor through **Device Properties** > **Performance Monitors** for that device.

To configure an SNMP active script performance monitor:

Step 1 In the web interface, go to **GO** > **Configure** > **Performance** > **Monitor Library**.

Step 2 In the Performance Monitor Library, click **New**.

Step 3 Select **Active Script** as the monitor type.

Step 4 In the Add Active Script Performance Monitor dialog, enter a name and a description for the monitor as it will appear in the Performance Monitor Library.

Step 5 Enter a number for the timeout (in seconds).

Step 6 Choose the type of script (JScript or VBScript) you will be using to write the monitor from the Script type drown-down list.

Step 7 Add a new variable to the Reference Variables list by clicking **Add**.

Note You can add up to 10 reference variables to the monitor.

Step 8 On the Add reference variables dialog box, enter a name and a description for the variable.

Step 9 Select SNMP from the object type drop-down list.

Step 10 If needed, adjust the timeout and retry counts for connection to the device.

Step 11 Click the **Browse (...)** button next to the Instance box. The SNMP MIB Browser appears.

Step 12 Enter the share name or IP address of the computer to which you are trying to connect.

Step 13 Enter the SNMP credential used to connect to the device (or click the **Browse (...)** button to access the Credentials Library to create a new credential.)

Step 14 If needed, adjust the timeout and retry counts for the computer to which you are trying to connect.

Step 15 Click **OK**. The SNMP MIB Walker appears.

Step 16 Use the navigation tree in the left pane to select the specific MIB you want to monitor. You can view more information about the property/value at the bottom of the dialog.

Step 17 Click **OK** to add the OID to the Performance counter and Instance boxes in the Add new reference variable dialog.

Step 18 Verify the configuration and click **OK** to add the variable to the Reference variable list on the Add active script performance monitor dialog.

Step 19 Type or paste your monitor code in the Script text box.

Step 20 Click **OK** to save changes and add the monitor to the Performance Monitor Library.

To configure a WMI active script performance monitor:

Step 1 In the web interface, go to **GO** > **Configure** > **Performance** > **Monitor Library**.

Step 2 In the Performance Monitor Library, click **New**.

Step 3 Select **Active Script** as the monitor type.

Step 4 In the Add Active Script Performance Monitor dialog, enter a name and a description for the monitor as it will appear in the Performance Monitor Library.

Step 5 Enter a number for the timeout (in seconds).

Step 6 Choose the type of script (JScript or VBScript) you will be using to write the monitor from the Script type drown-down list.

Step 7 Add a new variable to the Reference Variables list by clicking **Add**.

Note You can add up to 10 reference variables to the monitor.

Step 8 On the Add reference variables dialog box, enter a name and a description for the variable.

Step 9 Select SNMP from the object type drop-down list.

Step 10 If needed, adjust the timeout and retry counts for connection to the device.

Step 11 Click the **Browse (...)** button next to the Instance box. The SNMP MIB Browser appears.

Step 12 Enter the share name or IP address of the computer to which you are trying to connect.

Step 13 Enter the SNMP credential used to connect to the device (or click the **Browse (...)** button to access the Credentials Library to create a new credential.)

Step 14 If needed, adjust the timeout and retry counts for the computer to which you are trying to connect.

Step 15 Click **OK**. The SNMP MIB Walker appears.

Step 16 Use the navigation tree in the left pane to select the specific MIB you want to monitor. You can view more information about the property/value at the bottom of the dialog.

Step 17 Click **OK** to add the OID to the Performance counter and Instance boxes in the Add new reference variable dialog.

Step 18 Verify the configuration and click **OK** to add the variable to the Reference variable list on the Add active script performance monitor dialog.

Step 19 Type or paste your monitor code in the Script text box.

Step 20 Click **OK** to save changes and add the monitor to the Performance Monitor Library.

You can suspend or enable data collection on that monitor by selecting or clearing the checkbox next to the monitor name.

Example: Monitoring Router Bandwidth

Through the Performance Monitoring system, you can configure the application to gather bandwidth usage on your SNMP-enabled devices (routers, switches, and so on) and then track that usage through performance reports. Several performance monitors are installed with the application, but for bandwidth monitoring, the Interface Utilization monitor is the most useful because it shows percent utilization and throughput.

The Interface Utilization monitor gathers statistics on the volume of bytes going through the active interfaces on the device. You can collect data on all interfaces, active interfaces, or just specific interfaces. This monitor is configured and enabled through **Device Properties > Performance Monitors**.

Note Before you can configure the monitor, you must have SNMP-enabled on the device, and the proper credentials configured in the Credentials Library for the device. The Performance Monitoring system uses these credentials to connect to the device during the configuration process and during normal performance gathering. For more information on enabling SNMP, see Enabling SNMP on Windows Devices, page 10-2.

Configuring the Monitor

Because the Interface Utilization performance monitor is one of the default performance monitors installed with Cisco netManager, there is no global configuration required before setting up the monitor for the device itself. Once your SNMP credentials have been established for the device, you are ready to configure and enable the monitor to start gathering data.

Step 1 On the Cisco netManager web interface, select the device you want to gather performance data for and then right-click.

Step 2 Select **Properties** from the right-menu.

Step 3 Select **Performance Monitors** on the Device Properties dialog box.

Step 4 Select the Interface Utilization monitor from the list.

Step 5 Click **Configure** to set up the monitor for the device. Cisco netManager scans the device and discovers the interfaces on the device.

Once the scan is complete, the Configure Interface Data Collection dialog box appears. If the credentials for the device are not configured properly, the scan will fail (you can return to the Credentials Library to fix it.) If the device is not SNMP-enabled, the scan will fail (see Enabling SNMP on Windows Devices, page 10-2).

Step 6 Select the interfaces you want to collect data for. From the Collect data for drop-down list, select **All**, **Active**, or **Specific**. If you select Specific, select just the interfaces you want to monitor in the list. By default, active interfaces will be measured.

Step 7 (Optional) Click **Advanced** to change the retry and timeout settings for the SNMP connection to the device. Click **OK** to save the changes to the Advanced Settings.

Step 8 On the Configure Interface Data Collection dialog box, enter a time interval (in minutes) you want the application to wait between polls. The default is 10 minutes.

Step 9 Click **OK** to save the Interface Utilization configuration.

Viewing the Data

Cisco netManager takes several polling cycles before it has enough data to produce meaningful graphs (with a 10-minute poll interval, this may mean a few hours.) Once enough data has been gathered, there are several reports you can use to view this data:

- **By Device**—For device-specific data, view the Interface Utilization report (shown below); or the Device Status report, which shows graphical statistics of all monitors configured on a device.
- **By Group**—Access the Group Interface Statistics report to view summarized statistics for all devices in the selected group that have interface statistics enabled.
- **System Wide**—Use the Top 10 report to view the top performers in terms of bandwidth utilization across your network. You can also view system-wide data by running the Group Interface Utilization report against the All Devices dynamic group.

Example: Troubleshooting a Slow Network Connection

The real-time reporting provided by performance monitors can provide both the raw data and the data trend analysis that can help you isolate network problems. For example, you might experience a problem with a network connection between two of your office sites. This example shows how you can use performance monitors to troubleshoot the slow network connection.

Scenario:

A developer working in Augusta, Georgia, on an Atlanta-based project complains of a slow network connection between the Augusta and Atlanta offices. He states that it takes 40 minutes to check in files to the source library over the T1 connection.

The Atlanta office network administrator reacts by completing the following steps:

Step 1 On the Cisco netManager web interface, he goes to the Reports tab to select the Ping Response Time report.

Step 2 From here, he checks the connection from the Atlanta Cisco netManager application to the Augusta primary server. The report shows an increased response time beginning at 11:45 a.m.

Note The connection in this scenario has been configured with the appropriate performance monitors and has been gathering data for weeks. To set up this type of monitor for a connection, configure the Ping Latency and Availability monitor on a device located on the other end of the connection. For more information, see Configuring and Enabling Performance Monitors, page 10-3.

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.

CHAPTER 12

Using SNMP

Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a device (a host, gateway, server, and so on).

A monitoring or management application on the remote user's system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device provides information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the MIB. The MIB defines the SNMP objects that can be managed and the format for each object.

The SNMP protocol, together with the MIB, provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. The MIB information used by Cisco netManager is contained in MIB files in the MIB directory.

For basic steps on how to enable SNMP on a Cisco device, go to

http://www.cisco.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/dial_nms/snmpios.html#wp1049705

Monitoring SNMP Service

You can select SNMP on a device's **Services** dialog box (**Properties** > **Services**) and monitor it just as you can monitor any TCP service. SNMP monitoring checks to see if the SNMP service is running on the device.

Assigning SNMP Active Monitor to a Device

Step 1 In the Device Properties Active Monitor dialog box, click **Add**. The Active Monitor Properties dialog box opens.

Step 2 Select the SNMP Active Monitor, then click **Next**.

Step 3 Set the polling properties for the monitor, then click **Next**.

Step 4 Set up an Action for the monitor state changes.

Step 5 Click **Finish** to add the monitor to the device.

Note An SNMP-manageable device is identified on the map by a star in the upper-right corner of the device.

About the SNMP Agent or Manager

SNMP agent or manager software must be installed and enabled on any devices for which you want to receive SNMP information. Windows NT 4.0 and Windows 98, 2000, ME, and XP provide an SNMP agent. Network system manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

About the SNMP MIB

The MIB contains the essential objects that make up the *management information* for the device. The Internet TCP/IP MIB, commonly referred to as MIB-II, defines the network objects to be managed for a TCP/IP network and provides a standard format for each object.

The MIB is structured as a hierarchical object tree divided into logically related groups of objects. For example, MIB-II contains the following groups of objects:

- **System**. Contains general information about the device; for example, sysDescr (description), sysContact (person responsible), and sysName (device name).
- **Interfaces**. Contains information about network interfaces, such as Ethernet adapters or point-to-point links; for example, ifDescr (name), ifOperStatus (status), ifPhysAddress (physical address), ifInOctets, and ifOutOctets (number of octets received and sent by the interface).
- **IP**. Contains information about the processing of IP packets, such as routing table information; for example, ipRouteDest (the destination) and ipRouteNextHop (the next hop of the route entry).
- Other groups provide information about the operation of a specific protocol for example, tcp, udp, icmp, snmp and egp.
- The **enterprise** group contains vendor-provided objects that are extensions of the MIB.

Each object of the MIB is identified by a numeric object identifier (OID) and each OID can be referred to by its text label. For example, the system group contains an object named sysDescr, which provides a description of the device. The sysDescr object has the following object identifier:

iso.org.dod.Internet.mgmt.mib.system.sysDescr

1.3.6.1.2.1.1.1

This object identifier would be 1.3.6.1.2.1.1.1 to which is appended an instance subidentifier of 0. That is, 1.3.6.1.2.1.1.1.0 identifies the only instance of sysDescr.

All of the MIB-II objects (for TCP/IP networks) are under the MIB sub ree (so all these objects will have an identifier that starts with 1.3.6.1.2.1).

For a detailed description of the MIB, see RFC 1213.

About SNMP Object Names and Identifiers

Each SNMP object has a name and numeric identifier. For example, in the *system* group, the network object named *SysDescr* with object identifier 1.3.6.1.2.1.1.1 contains a description of the device.

An object can have one or more instances, depending on the configuration of the monitored device. For example, a device can have two network adapters, in which case there will be two instances of the *ifPhysAddress* object, which has object identifier 1.3.6.1.2.1.2.2.1.6. In this case, you need to specify an instance number at the end of the object identifier (such as 1.3.6.1.2.1.2.2.1.6.1). If you do not specify an instance, it defaults to zero.

About SNMP Operations

An SNMP application can read values for the SNMP objects (for monitoring of devices) and some applications can also change the variables (to provide remote management of devices). Basic SNMP operations include:

- **Get**. Gets a specified SNMP object for a device.
- **Get next**. Gets the next object in a table or list.
- **Set**. Sets the value of an SNMP object on a device.
- **Trap**. Sends a message about an event (that occurs on the device) to the management application.

The SNMP agent software on a device listens on port 161 for requests from an SNMP application. The SNMP agent and application communicate using User Datagram Protocol (UDP). Trap messages, which are unsolicited messages from a device, are sent to port 162.

Note If an SNMP application makes a request for information about a device but an SNMP agent is not enabled on the device, the UDP packets are discarded.

About SNMP Security

In Cisco netManager, credentials are used like passwords to limit access to a device’s SNMP data. The credentials system supports SNMPv1 and SNMPv2.

Credentials are configured and stored in the Credentials Library (found on the web interface menu at **GO > Configure > Credentials Library**) and used in several places throughout the application. They can be assigned to devices in **Device Properties > Credentials**, or through the Credentials Bulk Field Change option.

Devices need SNMP credentials assigned to them before SNMP-based Active Monitors will work.

Using the Trap Definition Import Tool

This tool lets you import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your Cisco netManager MIB folder: `\Program Files\Ipswitch\WhatsUp\Data\Mibs`.

The SNMP Trap monitors that are listed are based on one of three things:

- **Passive monitors already in the database**. By default, the passive monitor database comes with a few of the most Common SNMP traps already in it.
- **Passive monitors automatically created by** the Cisco netManager **Trap Definition Import Tool**. Use the Trap Definition Import Tool to create SNMP Traps from MIB files stored in `\Program Files\Ipswitch\WhatsUp\Data\Mibs` folder.
- **Passive monitors that you define yourself.** You can do this either by copying and pasting actual trap information directly from your existing logs, or by browsing the MIB for OID values that you are interested in and adding the Generic type (Major) and Specific type (Minor) information if required.

To import SNMP trap definitions into the Passive Monitor Library:

Step 1 In the Cisco netManager console, click **Tools > Trap Definition Import Tool**. The Trap Definition Import Tool dialog opens.

Step 2 Click to select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog opens and provides a message about the import results. Traps that already exist in the database are not imported again.

Configuring Global SNMP Timeout and Retry Settings

If an SNMP query does not respond in time, Cisco netManager will time out. It will then retry contacting the device for as many times as listed under the snmpretries attribute in the configuration file. The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, Cisco netManager waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry. The SNMP timeout and retries are global settings.

Step 1 Select **GO** > **Configure** > **Default SNMP Timeout**.

Step 2 Enter the following:

- **Timeout** (milliseconds)—Enter the timeout in milliseconds (ms). If a device does not respond to the scan within this time, the scan continues to the next IP address. The timeout should be set to 300 ms or greater.
- **Retry count**—This is the number of times to try to discover a device at a given IP address, before continuing to the next device.

CHAPTER 13

Administrative Tasks

This section provides information about various administrative information and tasks.

About Web Security

Cisco netManager is installed with the files needed to immediately begin connecting to the SSL web server using 128 bit encryption.

The files included with the install (root.pem and server.pem) are installed with every copy of Cisco netManager, therefore, your encrypted session may not be as secure as it could be.

These certificate files are installed for demonstration purposes only, and should be replaced with certificates that you generate and sign.

Furthermore, a sample certificate is issued with Cisco as the Common Name. This will always give a Domain Name Mismatch Security Error on every fresh browser session in your environment.

These sample files reside in the Cisco netManager `Install Directory>\data\SSL` directory and should be updated with your own files.

Configuring IP Security

To allow or deny access to Cisco netManager based on IP addresses:

Step 1 Select **GO** > **Configure** > **IP Security**.

Step 2 Complete the following:

Allow Hosts—IP addresses and ranges listed in Allow Hosts are granted access to Cisco netManager.

- To add a new IP address or range of IP addresses to this list, click **New**.
- To change an existing entry, click **Edit**.
- To remove an entry, select the entry, then click **Delete**.

Deny Hosts—IP addresses and ranges listed in Deny Hosts are denied access to Cisco netManager.

- To add a new IP address or range of IP addresses to this list, click **New**.
- To edit an existing entry, click its hyperlink in the IP Address column.
- To remove an entry, select it, then click **Delete**.

Step 3 Click **OK**.

Note Addresses which are neither on the allow nor the deny list are allowed. Addresses which are on both lists are allowed.

Stopping and Starting the Web Server

For troubleshooting purposes, the first thing you may want to try is to restart the web server. This stops and restarts all Cisco netManager processes. To stop and restart the web server:

Step 1 Select **Start** > **Programs** > **Cisco netManager 1.0** > **Daemons** > **Stop**. This stops the web server.

Step 2 Select **Start** > **Programs** > **Cisco netManager 1.0** > **Daemons** > **Start**. This restarts the web server.

Configuring the Web Server

You can edit the SSL and web server ports, session timeout (amount of time after which a session ends for an inactive user).

Note If you are using IIS as your Web server, the Up Web Server options are disabled.

Step 1 Select **GO** > **Configure** > **Manage Web Server**.

Step 2 Edit the web server information.

Configuring the Web Interface to use IIS

Follow these steps to run the Cisco netManager web interface through an Internet Information Services (IIS) web server.

Step 1 Stop the following services and applications:

- Cisco netManager Engine service
- Cisco netManager Web service
- Task Tray application

Step 2 Allow MSDE to use SQL Server Authentication. Use Regedit.exe to set:

```
HKEY LOCAL MACHINE\Software\Microsoft\Microsoft SQL
Server\WHATSUP\MSSQLServer\LoginMode=0
```

Step 3 Restart the MSSQL$WHATSUP service.

Step 4 Specify a username and password for Cisco netManager to use when connecting to MSDE:

a. Go to **Control Panel > Administrative Tools > Data Sources** and select the **System DSN** tab.

b. Select the Cisco netManager DSN and click **Configure**. The Configuration wizard appears.

c. Verify that the fields in the first dialog are correct and click **Next**.

d. In the second dialog, verify that the With SQL Server authentication using login ID and password entered by the user option is selected. In this same dialog specify user=`sa` and password=`wug_sa` and click **Next**.

e. In the third dialog, ensure that the first option is selected and Cisco netManager appears in the drop-down menu, and then click **Next**.

f. Continue to click **Next** until you come to the final dialog, and then click **Finish**.

Step 5 Stop IIS.

Step 6 Create a virtual directory in IIS named NmConsole which points to <Cisco netManager install path>\HTML\NmConsole\. Go to Windows **Control Panel** > **Administrative Tools** > **Internet Information Services**. Right-click **Default Web Site** and choose **New > Virtual Directory**. We strongly recommend that you name this new directory NmConsole.

Step 7 Enable parent paths for the default web site (to support use of the relative paths used to navigate in the Cisco netManager web interface).

a. Go to **Control Panel > Administrative Tools > Internet Information Services**.

b. In the IIS Manager, expand Web sites, then right-click the newly created NmConsole virtual directory and choose **Properties**.

c. On the Virtual Directory tab, click **Configuration**.

d. On the Options tab, select **Enable parent paths**. Click **OK**.

Step 8 Set authentication for the virtual directory you set up in Step 6. To do this:

a. In IIS Manager, right-click the virtual directory and select **Properties**, then select the **Directory Security** tab.

b. In **Anonymous access and authentication control**, click **Edit**. Enable anonymous access and set the username and password to a local administrator. Click **OK**.

Step 9 For IIS version 6:

In IIS Manager, select Web Service Extensions and allow Active Server Pages.

Step 10 Restart IIS.

Step 11 Set the internal web server to port 8080, or disable it. If you disable the Cisco netManager web interface, ensure that the reports still load correctly.

Step 12 Restart the services and applications you stopped in Step 1.

Step 13 Connect to the web interface by opening a browser and entering the following address in the Address box: http://ip_address/NmConsole/

Note If you receive a scanning-device error, see Resolving IIS Scanning-Device Error, page 13-4.

Resolving IIS Scanning-Device Error

There is a known issue with IIS when adding a device through IIS. You may receive an "error scanning device" message. There are two methods of resolving this issue:

- The simplest is to set the virtual directory to run under low application protection (http://support.microsoft.com/?id=326086). Use this if Cisco netManager is the only application using IIS.
- If you have other sites/services running in IIS, you'll need to change the account used to launch the Cisco netManager processes. Follow these steps:

Step 1 Open the Component Services control panel (**Start** > **Run** > **dcomcnfg.exe**).

Step 2 Navigate to the COM+ Applications folder (**Component Services** > **Computers** > **My Computer**).

Step 3 Right-click **IIS Out-Of-Process Pooled Applications** and choose **Properties**.

Step 4 Select the **Identity** tab and change the user in the This user section to an account with administrator access.

Step 5 Restart IIS (be sure to restart the entire IIS suite, not just the web services).

Step 6 For IIS 6 you will also need to change the account used for the Application Pool that Cisco netManager is using in IIS.

Step 7 Open the IIS manager (**Start** > **Run** > **inetmgr**).

Step 8 Browse to Application Pools, then right click **DefaultAppPool** and select properties.

Step 9 Select the **Identity** tab, set the Application Pool Identity to Configurable, then enter an account with administrator access and click **OK**.

Step 10 Restart IIS (be sure to restart the entire IIS suite, not just the web services).

Configuring LDAP

Step 1 Select **GO** > **Configure** > **LDAP Credentials...**.

Step 2 Enter the following:

- **LDAP Server**—Enter the hostname or IP address of your LDAP server. If you are authenticating to an Active Directory domain, the LDAP server for your domain is a domain controller (DC).
- **LDAP Port**—Enter the number of the port your LDAP server monitors for queries. For most LDAP configurations, the default value of 389 will work.
- **Authorize DN**—Enter the path to the container which holds the users you want to use as Cisco netManager users. See Authorize DN examples, page 13-5.
- **Secure**—Select if you want LDAP queries to be encrypted using SSL. Your LDAP server must be configured to accept SSL connections for this option to work.
- **Test**—Select to bring up the Test dialog box. The Test dialog box allows you to verify that your LDAP credentials are se tup correctly.

Note To enable LDAP credentials to work, you must configure users for those users that you would like to grant access to. These users must match the LDAP credentials you have configured.

Authorize DN examples

- Active Directory
  - If you are using Active Directory, you can authenticate any user on the domain (after setting up a Cisco netManager user which matches the Active Directory login name for that Active Directory user) using the following format. As an example, for the domain CISCOMGR, you would use:

    CISCOMGR%s
  - If you're using Active Directory, but only want to allow users from a specific container to log in, use the following format. As an example, if your user, Bandy Wendy, is in the container, \OU=Sites\OU=KUL\OU=Non-Developers, on the bigbluepuddle.org domain, you would use:

    CN=%s,OU=Non- Developers,OU=KUL,OU=Sites,DC=bigbluepuddle,DC=org

    These DN strings use the Active Directory login name as the Cisco netManager username.
- Standard LDAP Server
  - If you're not using Active Directory, you will need to specify the LDAP attribute and path to the container which holds the user objects you want to use. An example could be;

    CN=%s,OU=Users,o=yourdomain.net

    where %s is username/password information entered from their respective fields.

Note If you are unsure which LDAP attribute to use, or which path to specify, contact your LDAP administrator or LDAP vendor.

Managing Users

Administrators have read-write access privileges. They can manage and configure users, devices, device groups, reports, and notifications. They can also acknowledge and clear events. Guest users, by default, have read-only privileges. These users can verify operational status using topology displays, search for phone and device information, view operational alerts on devices and phones in the network, view all reports (except system reports), and modify workspace views. Administrators can modify a guest user's access privileges.

There is another user profile called Cisco_User that cannot be modified or deleted. Cisco_User has the same privileges as a guest user, except Cisco_User cannot modify the layout of workspace views, and they can view all reports (including system reports). Cisco_User becomes useful if users or administrators have made modifications to their workspace view (for example, accidentally deleting a report) and want to restore default settings. Administrators can view the default settings of Cisco_User and apply them to themselves or to other users.

Note Administrators can copy Cisco_User profile when creating new users.

The administrator can assign privileges to a user from the Manage Users dialog box.

Step 1 Select **GO** > **Configure** > **Manage Users...**.

Step 2 Click **Add** to create a new user or **Edit** to modify an existing user.

Step 3 Enter the name of the user in the User Name field.

Step 4 Select the method of authenticating the user:

- **Internal**. Use Cisco netManager's internal user database.
- **LDAP**. Use an external LDAP database.

Step 5 Enter the user's password (only if Authentication Type is set to Internal).

Step 6 Enter the user's password again in the Confirm Password field.

Step 7 From Home Group, select the device group that the user will see when they log into Cisco netManager’s web interface. If they have the correct group access rights, they will be able to navigate out of this group.

Step 8 From Device Group Settings, click Set Device Group Access Rights to make a change to which groups the user has read and write access to.

Note This section is only visible after a user has been created. After initial creation, you are prompted to set device group permissions.

Step 9 From User Rights, select which options to give the user access to:

- **Manage Users**—Create and edit users for the web interface. This option also allows users to specify device group and device access rights.
- **Manage IP Security**—Allows or refuses users access to the web interface to specific IP addresses.
- **Configure Active Monitors**—Configure active monitors for devices in the database.
- **Configure Passive Monitors**—Configure passive monitors for devices in the database.
- **Manage Groups**—Create, edit, or remove device groups, in the groups in which the user has access.
- **Access Group and Device Reports**—View group and device reports for the groups to which the user has access.
- **Access System Reports**—View system reports.
- **Configure LDAP Credentials**—Configure LDAP credentials for the web interface.
- **Configure Credentials**—Configure SNMP and Windows credentials.
- **Change Your Password**—Change their own password.
- **Configure Actions**—Create and edit actions in the Action Library.
- **Manage Devices**—Add new devices and edit existing devices in the groups in which the user has access.
- **Manage Web Server**—Change the configuration of the web server.
- **Manage Recurring Actions**—Create, edit, or remove Recurring Actions, in the groups in which the user has access.
- **Translations**—Translate Cisco netManager dialog boxes.
- **Configure Workspaces**—Configure workspaces in the web interface.
- **Configure Action Policies**—Create, edit, or remove Action Policies, in the groups in which the user has access.
- **Configure Performance Monitors**—Configure performance monitors for devices in the database.

- **Access Active Discovery Results**—Access active discovery results.
- **Manage Workspace Views**—Access the Workspace Library and manage workspace views.

Changing Admin Preferences (Password Change)

To change your user account preferences:

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

Step 2 Enter the following:

General

- **Language**—Select a language for the application.
- **Change your password—**Click this option to change your account password.

Refresh Intervals

- **Workspace report—**Enter a time (in seconds) for how often workspace reports should refresh.
- **Full report**—Enter a time (in seconds) for how often reports should refresh.
- **Devices tab**—Enter a time (in seconds) for how often the Devices tab should refresh.

Web Alarms

- **Enable Web alarms**—Check this box to enable Web alarms.
- **Check every**—If you enable Web alarms, enter a time (in seconds) for how often Cisco netManager should check for Web alarms.
- Click **OK**.

Using the Cisco netManager Console

There are a few tasks that cannot be performed via the Cisco netManager web interface. For these tasks, you must use the console. The console is available from the server where Cisco netManager is installed (**Start** > **All Programs** > **Cisco netManager 1.1** > **Cisco netManager 1.1 Discovery**).

Changing the Date and Time Format

To change the date and time format:

Step 1 From the Cisco netManager console, select **Configure** > **Program Options**.

Step 2 Select the **Regional** section.

For each of the three date formats, select the one that best suits your needs.

Step 3 Click **OK**.

These formats can be seen in use on several of the reports available on the Reports view.

Changing How Long Report Data Is Stored

Ping Active Monitor data is stored in the Cisco netManager database to populate the Performance reports available in the application.

Step 1 From the Cisco netManager console, select **Configure** > **Program Options**.

Step 2 In Program Options, select **Report Data**.

On the Report Data section, you can change the settings for raw data, hourly data, and daily data.

Step 3 Click **OK** to save the changes.

You can see how many rows in the database that the data takes up by viewing the numbers under the time settings.

Changing the Device State Colors or Icons

To change the device state colors or icons:

Step 1 From the Cisco netManager console, select **Configure** > **Program Options**.

Step 2 In Program Options, select **Device States**.

To change an existing icon or state, select the entry from the list and click **Edit**.

Step 3 Adjust the shape and color of the icon using the settings in the Device State Editor.

Step 4 Click **OK** to save changes.

If the default settings do not fit your needs, click **Add** to create a new device state, using the internal state and state time that you need.

Changing Clock or Regional Preferences

To use a 24-hour clock instead of the default 12-hour clock:

Step 1 From the Cisco netManager console, select **Configure** > **Program Options**.

Step 2 Select the **Regional** section.

Step 3 Select the **Use 24 hour clock** option.

Step 4 Click **OK**.

Managing Notifications

Notification configuration options are available through the system registry. The registry location where these options can be set is at

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco netManager\1.1

Notifications run as a separate service, CiscoNotificationService.exe, and it relies on NmService.exe to sense the events that happen on the system.

Configuring SMTP Load

The notification engine uses a thread pool to send out e-mail notifications. The number of threads that talk to the e-mail servers at the same time is controlled so that the servers do not overload. You can increase the number of threads to increase the throughput of e-mails sent or you can decrease the number of threads to reduce the load at the e-mail server.

Step 1 From the server where Cisco netManager is installed, select **Start > Run**.

Step 2 Enter **regedit**. The Registry Editor window appears.

Step 3 Navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco netManager\1.1 folder.

Double-click **notification_max_threads** to modify the number of threads.This key must be of type REG_DWORD and must have a minimum of 1 and a maximum of 500. The default value is 32.

Note The maximum number of threads is created only if there is a need; for example, if a flurry of events occurs in the system and causes many e-mails to be sent. But if the number of concurrent operations is higher than the number that your e-mail server can support, the SMTP server could drop connections, causing you to lose e-mail. (Failed e-mail send operations are retried a maximum of three times. All errors and e-mails sent are logged.)

Performance and E-Mail Details

The default e-mail configuration supports 75 e-mails per second to be sent in situations of extreme activity. This figure can be affected by the actual SMTP server used, SMTP server responsiveness, and conditions on the network. If your server can take a greater load, the figures can be improved by increasing the number of concurrent threads that are active in the thread pool, as described in Configuring SMTP Load, page 13-9.

Note

- Some antivirus products automatically scan outgoing e-mail, which can affect performance. See the appropriate antivirus product documentation to disable this option.
- It is good practice to create e-mail aliases rather than configuring several e-mail addresses. This allows for better mail delivery performance and also makes it easier to create several notification rules that use the same e-mail addresses.
- If multiple SMTP servers are configured as part of multiple rules, the concurrency figures will likely be lower than what is supported.

Configuring Socket Timeouts

The default socket timeouts for connection, read, and write can be controlled using registry keys created in the same location. The timeouts are not kept too high by default to avoid issues due to erroneous configurations. However, timeouts can be increased to deal with a slow network. They keys that control the timeouts are the following:

- connection timeout—notification_socket_connect_timeout (default 30)
- read timeout—notification_socket_read_timeout (default 10)
- write timeout—notification_socket_write_timeout (default 5)

Note All keys must be of type REG_DWORD and have a maximum of 50 and a minimum of 1.

Notification Logging

The default log files are created in the <cnm install folder>\logs. E-mail notification logs contain records of all e-mails sent and errors encountered when sending e-mail. The default filename is NotificationEmailApp.log.

Events that need to be sent out along with changes in the system configuration (rules devices groups) are processed by the Notification engine. A record of this activity can be found in CiscoNotificationFrameWorkApp.log.

Note If the default log levels are changed in the log configuration for these files, the messages will cease to appear.

APPENDIX A

Events Processed

The following tables list all possible events you might see in Cisco netManager, along with the following:

- Description—A summary of the event, including typical causes (if known).
- Trigger—How Cisco netManager learns of the event: from normal polling, a threshold that was exceeded, a diagnostic test result, a trap that was received, or an event received from Windows Event Manager.
- Severity—The severity that Cisco netManager assigns to the event: critical, warning, or informational.
- Device Type—The devices, as classified in Cisco netManager, on which the event can occur.

Lists of Events

The following tables provide descriptions of the events displayed. For specific events related to Cisco Unified Communications Manager Express, Cisco Unity Express, and *unresponsive* events, see the following tables:

- Table A-1 displays a list of common events for all devices.
- Table A-2 displays a list of Cisco Unified Communications Manager events.
- Table A-3 displays a list of Cisco Unified Communications Manager Express.
- Table A-4 displays a list of Cisco Unity events.
- Table A-5 displays a list of Cisco Unity Express events.
- Table A-6 displays a list of Local Wireless Access Point events.
- Table A-7 displays a list of SRST events.
- Table A-8 displays a list of active monitor events associated with the *unresponsive* Cisco netManager event.

For information on processed SNMP traps, see Appendix B, “Processed SNMP Traps and Corresponding Cisco netManager Events.”

Table A-1 Common Events

Event	Description	MIB
Fan Down	**Description:** Fan condition is down. **Severity**: Critical. **Device Type**: All	For MCS COMPAQ platform, CPQ-HEALTH-MIB For MCS IBM platform, UMSLMSENSOR-MIB For routers and switches, CISCO-ENVMON-MIB
Fan Degraded	**Description:** Fan condition is degraded. **Severity**: Warning. **Device Type**: All	For MCS COMPAQ platform, CPQ-HEALTH-MIB For MCS IBM platform, UMSLMSENSOR-MIB For routers and switches, CISCO-ENVMON-MIB
High CPU Utilization	**Description**: Current utilization exceeds the utilization threshold configured for this network adapter or processor. **Trigger**: Exceeded one of these thresholds: • Utilization Threshold. • Processor Utilization Threshold. **Severity**: Critical. **Device Type**: Host, media server, router, switch, optical switch, voice gateway, Wireless LAN Controller.	For MCS, HOST-RESOURCES-MIB For routers and switches, CISCO-PROCESS-MIB For wireless LAN controller, airspace.bsnSwitching.agentResourceInfoGroup
Insufficient Free Hard Disk	**Description**: Free disk space is low. **Trigger**: Exceeded Free Hard Disk Threshold. **Severity**: Critical. **Device Type**: Media server.	HOST-RESOURCES-MIB
Insufficient Free Physical Memory	**Description**: System is running out of physical memory resources. **Trigger**: Exceeded Free Physical Memory Threshold. **Severity**: Critical. **Device Type**: Voice gateway, Wireless LAN Controller.	For MCS, HOST-RESOURCES-MIB For routers and switches, CISCO-MEMORY-POLL-MIB. For wireless LAN controller, airspace.bsnSwitching.agentResourceInfoGroup
Insufficient Free Virtual Memory	**Description**: System is running out of virtual memory resources. **Trigger**: Exceeded Free Virtual Memory Threshold. **Severity**: Critical. **Device Type**: Media server.	HOST-RESOURCES-MIB

Table A-1 Common Events (continued)

Event	Description	MIB
Power Supply Down	**Description:** Power supply state is Down. **Trigger:** Trap. **Severity:** Critical. **Device Type:** Media server or voice gateway.	UMSEVENT MIB
Power Supply Degraded	**Description:** Power supply state is degraded. **Trigger:** Trap. **Severity:** Critical. **Device Type:** Media server or voice gateway.	UMSEVENT MIB
Temperature High	**Description:** Operating temperature exceeds the threshold. **Trigger:** Exceeded Relative Temperature Threshold. **Severity:** Critical. **Device Type:** Media server, router, or switch.	Cisco-Stack-MIB
Temperature Sensor Down	**Description:** Temperature sensor reports abnormal temperature measurements and reports its condition as failed. **Severity:** Critical. **Device Type:** Media server, router, or switch.	For MCS COMPAQ platform, CPQ-HEALTH-MIB For MCS IBM platform, UMSLMSENSOR-MIB For routers and switches, CISCO-ENVMON-MIB
Temperature Sensor Degraded	**Description:** Temperature sensor response is degraded. **Severity:** Critical. **Device Type:** Media server, router, or switch.	For MCS COMPAQ platform, CPQ-HEALTH-MIB For MCS IBM platform, UMSLMSENSOR-MIB For routers and switches, CISCO-ENVMON-MIB

Table A-1 Common Events (continued)

Event	Description	MIB
Unresponsive	**Description**: Device does not respond to ICMP or SNMP requests. Probable causes are: • On a system: ICMP ping requests and SNMP queries to the device timeout received no response. • On an SNMP Agent: Device ICMP ping requests are successful, but SNMP requests time out with no response. **Note** A system might also be reported as Unresponsive if the only link (for example, an interface) to the system goes down. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Host, hub, router, switch, optical switch, media server, phone access switch, voice mail gateway, or voice gateway.	—
Cold Start	**Description**: Cold Start. **Trigger**: Processed trap. **Severity**: Informational. **Device Type**: All.	RFC 1215
Warm Start	**Description**: Warm Start. **Cause**: Trap. **Severity**: Informational. **Device Type**: All.	RFC 1215
Link Down	**Description**: Link is down. **Cause**: Trap. **Severity**: Critical. **Device Type**: All.	RFC 1215
Card Down	**Description**: Card or module has been powered down or removed. **Trigger**: Polling, Traps **Severity**: Warning. **Device Type**: All that support CISCO-FRU-CONTROL.	CISCO-FRU-CONTROL-MIB ciscoMgmt.ciscoEntityFRUControlMIB.cefcMIBObjects.cefcModule.cefcModuleTable.cefcModuleTableEntry.cefcModuleOperStatus ciscoMgmt.ciscoEntityFRUControlMIB.cefcFRUMIBNotificationPrefix.cefcMIBNotifications.cefcModuleStatusChange

Table A-1 Common Events (continued)

Event	Description	MIB
Authentication Failure	**Description**: Unknown manager access. **Trigger**: Processed trap **Severity**: Warning. **Device Type**: All	RFC-1215
Voltage High	**Description:** Voltage on the device is high. **Cause:** Trap. **Severity:** Critical. **Device Type:** Media server, router, or switch.	UMSEVENT MIB

Table A-2 Cisco Unified Communications Manager Events

Event	Description	MIB
Communications Manager Down	**Description:** Cisco Unified Communications Manager can run but is not running due to some problem in the application or device. **Trigger:** Polling. **Severity:** Critical. **Device Type:** Media server.	SysAppl-MIB
Service Down	**Description**: Service can run but is not running due to some problem in the service or device. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media server.	SYSAPPL-MIB
Gateway Connectivity Lost	**Description:** A gateway has unregistered with a Cisco Unified Communications Manager. **Cause:** Logical topology. **Severity:** Critical. **Device Type:** All.	CCM-MIB
Media Connectivity Lost	**Description:** A Media application has lost connection with the Cisco Unified Communications Manager. **Cause:** Logical topology. **Severity:** Critical. **Device Type:** All	CCM-MIB

Table A-2 Cisco Unified Communications Manager Events (continued)

Event	Description	MIB
MPX Connectivity Lost	**Description:** An MPX has lost connection with the Cisco Univfied Communications Manager. **Cause:** Logical topology **Severity:** Critical. **Device Type:** All.	CCM-MIB
Unity Connectivity Lost	**Description:** Unity has lost registration with the Cisco Unified Communications Manager. **Cause:** Logical topology. **Severity:** Critical. **Device Type:** All.	CCM-MIB
CodeYellowEntry	**Description:** Cisco Unified Communications Manager has initiated call throttling due to unacceptably high delay in handling incoming calls. **Cause:** Trap processed as Syslog. **Severity:** Critical. **Device Type:** Cisco Unified Communications Manager.	CISCO-SYSLOG-MIB
CodeRedEntry	**Description:** Cisco Unified Communications Manager is not able to recover, even after attempting call throttling. The Cisco Unified Communications Manager service is shut down. **Cause:** Trap processed as Syslog. **Severity:** Critical. **Device Type:** Cisco Unified Communications Manager.	CISCO-SYSLOG-MIB

Table A-2 Cisco Unified Communications Manager Events (continued)

Event	Description	MIB
DBReplicationFailure	**Description:** Combined alarm for emergency and error situations. It indicates failure in IDS Replication. Requires database administrator intervention. **Cause:** Trap processed as Syslog. **Severity:** Critical. **Device Type:** Cisco Unified Communications Manager.	CISCO-SYSLOG-MIB
CoreDumpFileFound	**Description:** Indicates a core dump from any process on the Cisco Unified Communications Manager. **Cause:** Trap processed as Syslog. **Severity:** Critical. **Device Type:** Cisco Unified Communications Manager.	CISCO-SYSLOG-MIB

Table A-3 Cisco Unified Communications Manager Express Events

Event	Description	MIB
CCME Down	**Description:** The Cisco Unified Communications Manager Express application is down. This could be due to some problem in the application or device. **Trigger:** Polling. **Severity:** Critical. **Device Type:** Router.	Cisco-CCME-MIB
CCME Ephone Deceased	**Description:** The state of an ephone registered to Cisco Unified Communications Manager Express changed to deceased. **Trigger:** Processed trap. **Severity:** Warning.	Cisco-CCME-MIB ccmeEPhoneDeceased
CCME Ephone Login Failed	**Description:** An ephone login to Cisco Unified Communications Manager Express was rejected or failed. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeEphoneLoginFailed

Table A-3 Cisco Unified Communications Manager Express Events (continued)

Event	Description	MIB
CCME Ephone Registration Failed	**Description:** An ephone attempted to register with Cisco Unified Communications Manager Express and failed. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeEPhoneRegFailed
CCME Ephone Registrations Exceeded	**Description:** The total number of Ephones registered is exceeded and then dropped below threshold. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeEphoneUnRegThresholdExceed
CCME Key Ephone Registration Change	**Description:** Registration status changed for a key IP ephone with respect to Cisco Unified Communications Manager Express. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeKeyEphoneRegChangeNotif
CCME Status Change	**Description:** Cisco Unified Communications Manager Express enabled state has changed. **Trigger:** Processed trap **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeStatusChangeNotif
CCME Livefeed MOH Failed	**Description:** Cisco Communications Manager Express Music-on-hold (Moh) live feed has failed. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeLivefeedMohFailedNotif

Table A-3 Cisco Unified Communications Manager Express Events (continued)

Event	Description	MIB
CCME Maximum Conferences Exceeded	**Description:** If the maximum number of simultaneous three-party conferences supported by the Cisco Communications Manager Express is exceeded. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeMaxConferenceNotif
CCME Night Service Change	**Description:** If there is change in night service status on this device. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router or voice gateway.	Cisco-CCME-MIB ccmeNightServiceChangeNotif

Table A-4 Cisco Unity Events

Event	Description	MIB
Too Many Inbound Ports Active	**Description:** Percentage of active Cisco Unity inbound ports exceeded threshold. **Trigger:** Exceeded Active Inbound Ports Threshold. **Severity:** Critical. **Device Type:** Media server.	CISCO-UNITY-MIB
Too Many Outbound Ports Active	**Description:** Percentage of active Cisco Unity outbound ports exceeds threshold. **Trigger:** Exceeded Active Outbound Ports Threshold. **Severity:** Critical. **Device Type:** Media server.	CISCO-UNITY-MIB
Too Many Unity Ports Active	**Description:** Percentage of active ports exceeds threshold. **Trigger:** Exceeded Active Ports Threshold. **Severity:** Critical. **Device Type:** Media server.	CISCO-UNITY-MIB

Table A-5 Cisco Unity Express Events

Events	Description	MIB
CUE Application Status Change	**Description:** An application on Cisco Unity Express has come online or gone offline. **Trigger:** Processed trap **Severity:** Warning. **Device Type:** Router.	CUE-MIB ciscoUnityExpressApplAlert
CUE Storage Issue	**Description:** Notification when storage device degradation is excessive. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router.	CUE-MIB ciscoUnityExpressStorageAlert
CUE Security Issue	**Description:** Notification when a possible security issue is detected **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router.	CUE-MIB ciscoUnityExpressSecurityAlert
CUE NTP Issue	**Description:** Notification of a Network Time Protocol (NTP) error. **Trigger:** Processed trap. **Severity:** Warning. **Device Type:** Router.	CUE-MIB ciscoUnityExpressNTPAlert
CUE CCM Connection Lost	**Description:** Cisco Unity Express has lost connection with Cisco Unified Communications Manager. **Trigger:** Processed trap. **Severity:** Critical. **Device Type:** Router.	CUE-MIB ciscoUnityExpressCallMgrAlert
CUE Resource Exhausted	**Description:** A Cisco Unity Express resource has been exhausted. **Trigger:** Processed trap. **Severity:** Critical. **Device Type:** Router.	CUE-MIB ciscoUnityExpressRescExhausted

Table A-5 Cisco Unity Express Events (continued)

Events	Description	MIB
CUE Backup Failed	**Description:** Cisco Unity Express backup failed. **Trigger:** Processed trap. **Severity:** Critical. **Device Type:** Router.	CUE-MIB ciscoUnityExpressBackupAlert
High VM Capacity Utilization	**Description:** Percentage of voicemail minutes used in Cisco Unity Express exceeds the Capacity Utilization Threshold. **Trigger:** Exceeded Capacity Utilization Threshold. **Severity:** Critical. **Device Type:** Router.	CISCO-UNITY-EXPRESS-MIB

Table A-6 Local Wireless Access Point Events

Event	Description	MIB
LWAP Interface Channel Utilization High	**Description**: Lightweight Access Point (LWAP) Interface Channel Utilization is high. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Wireless LAN Controller.	AIRESPACE-WIRELESS-MIB airespace.bsnWireless.bsnAP.bsnAPIfLoadParametersTable
LWAP Administrative Status Disable	**Description**: Lightweight Access Point (LWAP) Administrative Status is disabled. **Trigger**: Polling. **Severity**: Informational. **Device Type**: Wireless LAN Controller.	AIRESPACE-WIRELESS-MIB airespace.bsnWireless.bsnAP.bsnAPTable
LWAP Down	**Description:** Lightweight Access Point (LWAP) is powered down or unreachable. **Trigger**: Polling, trap. **Severity**: Critical. **Device Type**: Wireless LAN Controller.	AIRESPACE-WIRELESS-MIB airespace.bsnWireless.bsnTRAPs.bsnAPDisassociated

Table A-7 SRST Router Events

Event	Description	MIB
SRST Router Failure	**Description**: A catastrophic failure occurred on an SRST router. **Trigger**: Processed trap. **Severity**: Critical. **Device Type**: Router or voice gateway.	Cisco-SRST-MIB

Table A-8 List of Unresponsive Cisco netManager Active Monitor Events

Event	Description	MIB
Unresponsive	This event corresponds to an active monitor event. If these active monitors are enabled, then an event will appear if it fails. **Note** Ping and SNMP are enabled by default. The component column lists the actual monitor name: • DNS—Domain Name Service • Ping—Test accessibility • SNMP—Test accessibility of SNMP • Echo—TCP Echo Monitor • FTP—File Transfer Protocol (FTP server) • HTTP—Hypertext Transfer Protocol (web server) • HTTP Content—HTTP Content Monitor • IMAP4—Internet Message Access Protocol V4 • NNTP—Network News Transfer Protocol • POP3—Post Office Protocol V3 • Radius—Radius Monitor • SMTP—Simple Mail Transfer Protocol (e-mail server) • Time—Time server (RFC 868) • Telnet—Telnet protocol • Interface—SNMP interface monitor • HTTPS—Secure Hypertext Transfer Protocol (web server)	—

APPENDIX B

Processed SNMP Traps and Corresponding Cisco netManager Events

This section lists the traps that Cisco netManager processes and the events that Cisco netManager generates for each trap. For information on Cisco netManager events, see Appendix A, "Events Processed.".

Processed Standard SNMP Traps (RFC 1215)

SNMP Trap	Corresponding Cisco netManager Event
Cold Start	Cold Start Cisco Event
Warm Start	Warm Start Cisco Events
Link Up Link Down	Flapping—Link Down trap raises the event, and the Link Up trap clears the event

Processed CISCO-UNITY-EXPRESS-MIB Traps

SNMP Trap	Corresponding Cisco netManager Event
ciscoUnityExpressApplAlert	CUE Application Status Change
ciscoUnityExpressStorageAlert	CUE Storage Issue
ciscoUnityExpressSecurityAlert	CUE Security Issue
ciscoUnityExpressCallMgrAlert	CUE CCM Connection Lost
ciscoUnityExpressRescExhausted	CUE Resource Exhausted
ciscoUnityExpressBackupAlert	CUE Backup Failed
ciscoUnityExpressNTPAlert	CUE NTP Issue

Processed CISCO-CCME-MIB Traps

SNMP Trap	Corresponding Cisco netManager Event
ccmeEPhoneDeceased	CCME Ephone Deceased
ccmeEphoneLoginFailed	CCME Ephone Login Failed
ccmeEPhoneRegFailed	CCME Ephone Registration Failed
ccmeEphoneUnRegThresholdExceed	CCME Ephone Registrations Exceeded
ccmeKeyEphoneRegChangeNotif	CCME Key Ephone Registration Change
ccmeLivefeedMohFailedNotif	CCME Livefeed MOH Failed
ccmeMaxConferenceNotif	CCME Maximum Conferences Exceeded
ccmeNightServiceChangeNotif	CCME Night Service Change
ccmeStatusChangeNotif	CCME Status Change

Processed CISCO-SRST-MIB Traps

SNMP Trap	Corresponding Cisco netManager Event
csrstFailNotif	SRST Router Failure

APPENDIX C

Open Source License Acknowledgements

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, and so on, code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

INDEX

Symbols

% variables 6-18

A

access rights
- assigning to users 13-5
- device group 2-23

acknowledging
- events 2-2, 2-33, 13-5
- privilege required for 13-5
- state change 2-33, 6-23

action
- action policy, compared to 6-2
- applied report, description 11-10
- configuring 6-3
- deleting 6-15
- device, assigning to 6-15
- e-mailing 6-23
- library 6-2
- log report, description 11-10
- monitor, assigning to 6-16
- preventing, on a device 6-23
- recommendations for configuring 6-2
- suspending 6-17
- testing 6-15
- triggering 6-1

Action Builder Wizard, launching 6-4

action policy
- action, compared to 6-2
- creating 6-21
- custom, creating 6-21
- editing 6-22
- implicit 6-22
- recommendations for configuring 6-2

active discovery log report, description 11-9

active monitor
- availability report, description 11-9
- device, assigning to 8-3
- library 8-2
- outage report, description 11-10
- polling 5-3
- types 8-2
- *See also* Active Script Monitor

Active Script Monitor
- context code, example 8-15
- context object, using 8-21
- JScript, using 8-14
- library 8-14
- overview 8-14
- VBScript, using 8-14

activity log report, description 11-11

administration pages, launching from Service Level View 4-13

Administrator user 1-3

Alert Details page
- *See also* events processed by Operations Manager

all IP phones/lines report, description 11-11

assigning
- action to device 6-15
- action to monitor 6-16
- active monitor to device 8-3
- passive monitor to device 9-3

attributes, adding to device 2-13

audience for this document i-xiii

authentication method, user 13-5

authorization and tools 4-13

B

beeper action
- creating 6-4
- port settings 6-5

blackout period, scheduling 6-17

C

cautions
- active monitor type, deleting 8-4
- significance of i-xiv

changing
- device IP address 2-14
- device types 2-32
- IP address 2-14
- polling method 5-1

chassis inventory report, description 11-11

Cisco event history report, description 11-15

Cisco netManager web security 1-8, 13-1

Cisco Unity ports 11-34

cloning a notification group 7-4

configuring
- action 6-3
- action policy 6-21
- active monitor 8-3
- groups, dynamic 2-17
- groups, static 2-16
- listeners 9-1
- passive monitors 9-2
- performance monitors 10-3
- recurring reports 11-40
- SNMP monitor 10-7
- workspaces 3-4

conventions in this document, typographical i-xiii

CPU utilization
- report, description 11-12
- workspace content 3-9

credentials
- SNMP 2-30
- Windows 2-30

custom
- links, device property 2-31
- performance monitor
  - adding 10-6
  - report, description 11-12
  - workspace content 3-10

customizing workspace content 3-21

D

data collection
- IP phone 11-21
- performance monitors, enabling 10-3
- purging 11-2
- rolling up 11-2
- *See also* discovery

data retention, IP phone 11-21

deleting
- action 6-15
- active monitors 8-4
- notification group 7-5

dependencies
- down 5-3

example 5-2

setting 5-3

up 5-3

viewing 5-4

device

action, assigning to 6-15

adding 2-4

attributes, adding 2-13

error adding 2-4

IP address, changing 2-14

name, changing 2-14

network interfaces, adding 2-12

notes, adding 2-13

reports, list of 11-5

type, changing 2-32

workspace content 3-11

See also device groups and device properties

Device Discovery

using 2-7

using the wizard 2-6

device groups

dynamic groups, configuring 2-17

renaming 2-17

static groups, configuring 2-16

user-defined, creating 2-17

device import status report, description 11-13

device properties

action 2-29

credentials 2-30

notes 2-31

passive monitor 2-29

Devices

adding with Device Discovery wizard 2-6

discovering 2-6

devices report, description 11-14

device status

report, description 11-13

workspace, starting, from Service Level View 4-12

Device Tab, overview 2-2

disabling

action 6-17

active monitors 8-4

polling, dependencies and 5-2

discovery

active discovery log report 11-9

device 2-2

in My Network tree 2-2

phone 2-9

status 11-14

disk utilization

report, description 11-14

workspace content 3-12

DNS Monitor 8-2

documentation i-xiv

audience for this i-xiii

obtaining i-xv

typographical conventions in i-xiii

down dependency 5-3

dynamic device group, configuring 2-17

E

editing

action policy 6-22

workspaces 3-5

e-mail

action, creating 6-6

action, example 6-23

recurring reports, sending 11-40

suspending 6-17

enabling

client-side JavaScript 11-38

performance monitor 10-3

polling, dependencies and 5-2

SNMP, on Windows devices 10-2

encryption and security 1-8, 13-1

error, adding to device 2-4

error log report

passive monitor 11-27

performance monitor 11-27

event

acknowledging 2-2, 2-33

history 11-15

report, description 11-16

events

processed by Operations Manager, descriptions and triggers A-1

Expect keyword

regular expressions, testing 8-7

variations 8-7

See also script syntax 8-7

exporting reports 11-38

Expression Editor 8-6

See also script syntax

F

fan status

report, description 11-17

workspace content 3-13

favorites, adding reports to 11-39

find phone, in Service Level View 4-3

flash devices inventory report, description 11-16

flash files inventory report, description 11-16

flow control keyword 8-8

See also script syntax

G

general

error log report, description 11-17

reports, list of 11-5

group

dynamic 2-17

reports, list of 11-5

static 2-16

system-defined 2-15

user-defined 2-17

Guest user 1-3

H

health report, description 11-17

Home Page View 3-2

HomeSpace workspace 3-1

home workspace report, description 11-18

I

icons

device 4-8

device state 2-4

links 4-11

implicit action policy 6-22

importing

devices 2-14

trap definitions, SNMP 12-4

installing SNMP agent or monitor

procedure 10-2

requirement 12-2

interface

configuring on a device 2-12

details report, description 11-18

status 11-18

utilization

report, description 11-19

top 10 devices report 11-34

workspace content 3-13

inventory workspace content 3-14

IP address, changing 2-14

IP phone

discovery 2-9

lines per group report, description 11-25

move report, description 11-23

registration status 11-21

removed 11-21

report, description 11-30

unregistered 11-35

IP phones, associated with

Cisco Unified Communications Manager 4-12

Cisco Unified Communications Manager Express 4-12

IPX device, support for 5-4

J

JScript, using in Active Script Monitor 8-14

L

library

action 6-2

active monitor 8-2

Active Script Monitor 8-14

performance monitor 10-2, 10-6

listeners, passive monitor, configuring 9-1

log

recurring action report 11-29

SNMP trap 11-31

web user activity 11-36

Windows event 11-36

M

MAC address, duplicate, phone 11-21

maintenance mode

polling, disabling 5-2

scheduling 5-2

map display

dependencies, viewing 5-4

Service Level View 4-4

memory utilization

report, description 11-25

workspace content 3-15

menus

creating custom context 2-33

meta-characters *See* regular expression and script syntax

MIBs

about 12-2

folder, in Cisco netManager 12-4

Microsoft Word C-1

modem settings 6-5

module inventory report, description 11-26

monitor

- action, assigning to 6-16
- overview 8-1
- SNMP active script performance monitor 10-8
- status 11-17, 11-18
- *See also* active monitor, Active Script Monitor, passive monitor, performance monitor

N

navigating

- reports 11-39
- user interface 1-4
- workspaces 3-7

network

- interface, configuring 2-12
- tools, launching 4-13
- troubleshooting
  - example 10-14
  - using performance monitors to 10-14
  - using reports to 11-1

network tools from 4-13

note, adding to device 2-13

notifications 7-1

- cloning 7-4
- configuring 7-2
- configuring options 13-9
- configuring SMTP load 13-9
- configuring socket timeouts 13-10
- deleting 7-5
- e-mail details 13-9
- filtering 7-1
- logging 13-10
- managing 13-9
- performance details 13-9
- viewing 7-5

O

object names and identifiers, SNMP 12-3

obtaining documentation i-xv

overview

- dependencies 5-3
- product 1-1, 13-1

P

pager action

- creating 6-6
- port settings 6-5

passive monitor

- action, assigning to 6-16
- configuring 2-29, 9-2
- error log report, description 11-27
- listeners, configuring 9-1
- using passive monitor library 9-2

password, user, updating 13-5

percent variables, using 6-9

- beeper action 6-4
- e-mail action 6-6
- pager action 6-6
- program action 6-10
- SMS action 6-7

performance monitor

- configuring 10-13

custom, adding to library 10-6

data, viewing 10-13
device properties 2-26
enabling 10-3
error log report, description 11-27
router bandwidth example 10-12
SNMP active script, configuring 10-8
performance reports, list of 11-5
performance workspace content
historic 3-16
last poll 3-16
phone report, launching from Service Level View 4-12
ping
availability report, description 11-28
availability workspace content 3-17
response time report 11-29
Ping Monitor 8-2
Polling
starting and stopping service 5-2
polling 5-1
active monitors 5-2
dependencies 5-3
device property 2-30
disabling 5-2
interval, setting 5-2
maintenance mode, significance of 5-2
method, changing 5-1
protocol 5-1
starting and stopping 5-2
port
conflict, resolving 9-3
settings
beeper action 6-5
pager action 6-5

Unity details 11-34
power supply status
workspace content 3-18
printing reports 11-38
problem area
reports, list of 11-5
workspace panes 3-2
product overview 1-4
program action, creating 6-10
Program Options
changing Clock/Regional preferences 13-8
setting Web Server options 13-2
properties
group 2-16
purging data, schedule for 11-2

R

receiving SNMP traps 9-3
recurring
action log report, description 11-29
report log report, description 11-30
reports
configuring 11-40
e-mailing 11-40
testing 11-41
regular expression
rules, testing 8-7
syntax 8-11
See also script syntax
renaming
device 2-14
device group 2-17

setting Report Data storage time 13-8

reports

date range, changing 11-39

examples C-1

exporting 11-38

favorites, adding to 11-39

navigating 11-39

printing 11-38

saving 11-38

zoom tool, using 11-39

response time

ping, report 11-29

top 10 devices 11-34

workspace content 3-17

S

scheduling

blackout period 6-17

maintenance 5-2

script syntax

about 8-6

example

disconnect string 8-11

send to disconnect 8-11

text string 8-13

Expression Editor 8-6

regular expression 8-11

Telnet 8-14

See also Active Script Monitor

Security

starting and stopping the secure web server 13-8

security

about SNMP 12-3

certificate 1-8, 13-1

web 1-8, 13-1

send keyword 8-9

See also script syntax

Server

starting and stopping polling 13-2

starting and stopping the secure web server 13-8

starting and stopping the web server 13-2

service, SNMP, monitoring on device 12-1

Service Level View

illustration and description 4-2

launching 4-13

administration pages from 4-13

detailed information pages from 4-11

Device Status workspace from 4-12

exernal applications from 4-11

link status 4-11

starting 4-2, 4-7

topology

logical 4-1

physical 4-5

setting

dependencies 5-3

polling frequency 5-2

thresholds 3-20

Short Message Service *See* SMS

significance of cautions i-xiv

SimpleExpect keyword 8-10

See also script syntax

SMS action, creating 6-7

SNMP

agent or manager, installing 12-2

enabling, on Windows devices 10-2

Management Information Base (MIB) 12-2
monitor, configuring 10-7
object names and identifiers 12-3
operations 12-3
security 12-3
service, monitoring on a device 12-1
trap log report, description 11-31
traps, processed
CISCO-CCME-MIB traps B-2
CISCO-SRST-MIB traps B-2
CISCO-UNITY-EXPRESS-MIB traps B-1
standard SNMP traps (RFC 1215) B-1
traps, receiving 9-3
SNMP Monitor
configuring 10-9
definition 8-2
using, example 8-5
sound action, creating 6-8
SRST status 4-4
SSL and security 1-8, 13-1
stack inventory report, description 11-31
starting Action Builder Wizard 6-4
state change
acknowledgement report, description 11-32
acknowledging 2-33, 6-23
action, triggered due to 6-1
timeline report, description 11-32
state summary report, description 11-33
static device group, configuring 2-16
status
device import 11-13
device state icons 2-4
discovery 11-14
fan 11-17
interface 11-18
link 4-11
monitor 11-17, 11-18
phone registration 4-4
SRST 4-4
suspending
actions 6-17
notification 6-17
syntax *See* script syntax
Syslog
action, creating 6-9
entries report, description 11-33
system reports, list of 11-5

T

TCP/IP Monitor 8-2
Telnet, using in script 8-14
Telnet Monitor 8-2
temperature
statistics report, description 11-34
status workspace content 3-19
testing
action 6-15
recurring reports 11-41
text-to-speech action, creating 6-10
threshold
configuring 3-20
workspace content 3-19
time zone, and IP phone reports 11-21
top 10
report, description 11-34

workspace content 3-20

topology
  logical 4-1
  physical 4-5
Trap Definition Import Tool 12-4
traps
  definitions, importing 12-4
  SNMP, receiving 9-3
traps, processed and pass-through B-1
  processed SNMP traps
    CISCO-CCME-MIB traps B-2
    CISCO-SRST-MIB traps B-2
    CISCO-UNITY-EXPRESS-MIB traps B-1
    standard SNMP traps (RFC 1215) B-1
typographical conventions in this document i-xiii

U

Unity port utilization report, description 11-35
unregistered IP phone report, description 11-35
up dependency 5-3
user
  authentication method for, setting 13-5
  configuring 13-5
  password 13-5
  types 13-5
utilization
  CPU 11-12
    workspace content 3-9
  disk 11-14
  interface 11-19
  memory 11-25
  top 10 devices 11-34
  Unity port 11-35

V

variables, percent 6-18
VBScript, using in Active Script Monitor 8-14
viewing
  notification group 7-5
viewing dependencies 5-4
voice
  gateway details report, description 11-35
  services details report, description 11-36

W

web
  security 1-8, 13-1
  user activity log report, description 11-36
Web Server
  starting and stopping the secure web server 13-8
  starting and stopping the web server 13-2
WhatsUp Gold web security, about 1-8, 13-1
Windows Event Log
  listener, enabling 11-36
  report, description 11-36
WipPopup action, creating 6-9
wireless LWAP channel utilization report, description 11-37
wireless LWAP summary report, description 11-37
WMI monitor, configuring 10-9
workspace
  creating 3-5
  definition 3-1
  Device Status 3-2
  editing 3-5

HomeSpace 3-1
managing 3-4
navigating 3-7
problem areas 3-2
See also workspace content
workspace content
categories 3-8
customizing 3-21
moving 3-21
removing 3-21
types 3-9
types of information 3-8