

NetCentral

TV FACILITY MONITORING SYSTEM

User Guide

SOFTWARE VERSION 4.0

071-8338-00
JUNE 2004

the most watched worldwide

Copyright

Copyright © 2004 Thomson Broadcast and Media Solutions, Inc. All rights reserved. Printed in the United States of America.

This document may not be copied in whole or in part, or otherwise reproduced except as specifically permitted under U.S. copyright law, without the prior written consent of Thomson Broadcast and Media Solutions, Inc., P.O. Box 59900, Nevada City, California 95959-7900

Trademarks

Grass Valley, Profile, and Profile XP are either registered trademarks or trademarks of Thomson Broadcast and Media Solutions, Inc. in the United States and/or other countries. Other trademarks used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products. Thomson Broadcast and Media Solutions, Inc. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Thomson Broadcast and Media Solutions, Inc. trademarks and other proprietary rights may be found at www.thomsongrassvalley.com.

Disclaimer

Product options and specifications subject to change without notice. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Thomson Broadcast and Media Solutions, Inc. Thomson Broadcast and Media Solutions, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

U.S. Government Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7013 or in subparagraph c(1) and (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19, as applicable. Manufacturer is Thomson Broadcast and Media Solutions, Inc., P.O. Box 59900, Nevada City, California 95959-7900 U.S.A.

Revision Status

Rev Date	Description
December 17, 1999	Initial Release. Part # 071-0686-00
February 15, 2001	Revised to include new NetCentral II features. Part # 071-0686-01
July 17, 2002	Revised to include new tools, Facility view, log views, trap configuration, security, and other NetCentral III features. Part # 071-0686-02
June 11, 2003	Revised to include version 3.1 changes including Actions wizard, Filter Message wizard, and HTML editor. Part # 071-0686-03.
June 2, 2004	Revised to include version 4.0 changes. Part # 071-8338-00.

Contents

	Preface	9
	About documentation for the NetCentral system.....	10
	Using this manual.....	11
	About documentation for NetCentral Lite	12
	Grass Valley Product Support	13
	Web Technical Support	13
	Phone Support.....	13
	Authorized Support Representative.....	13
Chapter 1	Overview of the NetCentral system	
	System summary.....	16
	What NetCentral does	17
	How NetCentral works.....	18
	Architecture of NetCentral	18
	Components of NetCentral	19
	NetCentral core software	19
	Device providers	19
	Action providers	19
	HTML files with active drawings	19
	Technologies NetCentral uses	20
	Simple Network Management Protocol	21
	Syslog.....	22
	.Net	22
	FTP	22
	SQL	22
	XML	23
	Hypertext Markup Language	23
	Active drawings	23
Chapter 2	Installing the NetCentral system	
	Preparing for installation.....	25
	Installation overview	26
	Installation checklist.....	27
	Facility requirements	28
	NetCentral server requirements	28
	About the IP address of a NetCentral server	29
	NetCentral client requirements	29
	Monitored device requirements	30
	Verify and record network settings	30
	Installing software.....	31
	Installing NetCentral software on the server.....	31
	Installing NetCentral software on clients	32
	Reinstalling NetCentral software	33
	Uninstalling NetCentral software	33
	Installing device provider software	33
	Uninstalling device provider software	35
	Getting started.....	36
	Opening NetCentral manager for initial setup	36
	Auto-discovering devices.....	37
	Restart SNMP services on monitored devices	38
	Verify SNMP trap messages from monitored devices	38
	Set SNMP trap destinations on monitored devices	39
	Adding and removing devices	40
	Adding devices to the Tree view	41
	Removing devices from the Tree view.....	42

Accomplish other device-specific preparations	42
Monitoring with multiple protocols	42
How Syslog works in NetCentral	42
Setting up and using Syslog in NetCentral	43
Chapter 3 Monitoring with the NetCentral system	
About NetCentral monitoring	46
Accessing NetCentral	47
About access permissions	47
Starting NetCentral	47
Logging on and off of NetCentral	48
Accessing NetCentral manager from a remote location	48
Stopping NetCentral	48
Adding NetCentral to startup	49
Overview of the NetCentral main window	50
Viewing information in the NetCentral main window	51
Displaying the Facility view	52
Displaying the Messages view	53
Displaying the Graphs view	53
Displaying the Actions view	54
Displaying views in multiple windows	54
Refreshing the information area	54
Arranging the Tree view	55
Searching for a folder in the Tree view	56
Creating a Facility graphical view	57
Interpreting status indicators	60
About status indicators	60
Locating status indicators in the NetCentral main window	61
Interpreting grayed-out devices	61
Viewing status in the system tray icon	62
Responding to messages and actions	63
Interpreting NetCentral messages	63
Acknowledging messages	64
Clearing acknowledged messages	64
Clearing alarms	64
Clearing warning and critical icons	65
Finding monitored devices	66
Searching for a device	66
Viewing a simple list of devices	66
Browsing device status	67
Viewing subsystem properties	67
Viewing general information for a device	67
Researching device status in NetCentral messages	69
Researching messages	69
Defining messages displayed	70
Rearranging message information	71
Grouping messages	71
Searching messages	72
Exporting NetCentral messages	73
Setting the export view	73
Exporting messages	74
Defining an export query	75
Printing messages	76
Researching device status with graphs	77
Viewing statistical graphs	77
Defining information graphed	78
Researching device-specific logs	79

	Viewing a single device-specific log	79
	Downloading multiple device-specific logs	80
	Using device-specific features	82
	Viewing version information	82
Chapter 4	Managing messages and actions	
	About messages and actions	84
	Configuring messages	85
	Adding remarks to messages	85
	Adding or editing a remark	85
	Copying messages	86
	Configuring actions and notifications	87
	Adding and modifying actions	87
	Adding actions for devices	87
	Adding an action for a folder	89
	Adding an action for a subsystem	89
	Adding an action for a message	89
	Modifying or removing an action	90
	Setting default action settings	91
	Sending e-mail and pager notifications	91
	Configuring properties for sending unscheduled e-mail	92
	Configuring properties for sending scheduled e-mail	92
	Playing a sound file	94
	Configuring properties for playing an audio file	94
	Playing a beep	95
	Configuring properties for playing a beep	95
	Running a program	96
	Configuring properties for running a program	96
	Launching a URL	98
	Configuring properties for launching a URL	98
	Using other actions	99
	Filtering messages to disable actions	100
	Filtering messages by device	100
	Filtering messages by folder	101
	Filtering messages by subsystem	102
	Filtering a displayed message	102
Chapter 5	Administering the NetCentral system	
	Using the Application Logs Viewer	104
	Adding devices	104
	About the discovery process	104
	Manually adding a device	105
	Configuring Auto-discovery to add devices	106
	Removing devices	108
	Setting automatic SNMP trap configuration	109
	Setting heartbeat polling	111
	Managing NetCentral security	113
	Setting up NetCentral security levels and user groups	113
	Logging on to NetCentral manager	114
	Setting access rights to NetCentral manager features	114
	Access rights to NetCentral device-specific features	116
	Managing port access	116
	Backing up the NetCentral database	117
	Accommodating NetCentral database growth	118
	Setting up for remote access	118
	Verifying components installed and running	118
	Connecting a NetCentral client to a different NetCentral server	120

	Adding custom tools	120
Chapter 6	Troubleshooting the NetCentral system	
	Characterizing the problem	123
	When does the problem occur?	123
	What is the behavior that indicates the problem?	123
	Where does the problem occur?	123
	What has changed?	124
	Diagnosing NetCentral problems	124
	About the NetCentral Diagnostic tool	124
	Running diagnostic tests on NetCentral components	124
	Running diagnostic tests on a monitored device's SNMP agent.....	126
	Generating a list of all SNMP trap messages.....	127
	About logs that contain NetCentral system information	128
	Restarting NetCentral services	128
	NetCentral troubleshooting guide	129
Appendix A	Graphical view tutorial	
	Preparations	133
	Prerequisite skills and system requirements	133
	Requirements	134
	Design	134
	Resources	134
	Propagating the Graphical view to NetCentral client PCs	134
	Creating a custom view of monitored devices.....	135
	Adding subsystem indicators	137
	Executing a program	140
	Applying an annotation layer.....	142
	Placing a folder icon onto the HTML page	142
Appendix B	Simple Network Management Protocol tutorial	
	Introduction to SNMP	143
	SNMP Basic Components	143
	SNMP Basic Commands	144
	SNMP Management Information Base	145
	SNMP and Data Representation	146
	SNMP Version 1	146
	SNMPv1 and Structure of Management Information	146
	SNMPv1 and ASN.1 Data Types	147
	SNMPv1 and SMI-Specific Data Types.....	147
	SNMP MIB Tables	147
	SNMPv1 Protocol Operations	148
	SNMPv1 Message Formats	148
	SNMPv1 Message Header	148
	SNMPv1 Protocol Data Unit	148
	Trap PDU Format	149
	SNMP Version 2.....	149
	SNMPv2 and Structure of Management Information	149
	SMI Information Modules	150
	SNMPv2 Protocol Operations	150
	SNMPv2 Message Format	150
	SNMPv2 Message Header	150
	SNMPv2 Protocol Data Unit	151
	GetBulk PDU Format.....	151
	SNMPv2 Trap PDU Format.....	153
	SNMP Version 3.....	153
	What SNMPv3 Covers?	153

	SNMPv3 Message Format	155
	NetCentral as Trilingual Network-Management System.....	156
	What is a Trilingual Network-Management System?.....	156
	Design of NetCentral SNMP Service and Communication	157
	Processing traps in NetCentral SNMP Service	157
	What Libraries to Use?	158
	Categories of SNMP Libraries	158
	Some of WINSNMP Libraries	158
	Some of open source Libraries and their Limitations	159
	References	159
Appendix C	Examples of typical NetCentral systems	
	Monitoring an Open SAN that uses PFC500 RAID storage	162
	Monitoring an Open SAN that uses PFR500 RAID storage	163
	Monitoring Profile XP Media Platforms.....	164
Appendix D	Examples of Windows procedures	
	Installing SNMP service on Windows 2000	165
	Setting SNMP trap destinations on Windows 2000	166
	Glossary	169
	Index	173

Preface

This manual documents the full-featured NetCentral manager product, as explained in the following sections.

- [“About documentation for the NetCentral system” on page 10](#)
- [“Using this manual” on page 11](#)

If you are using the NetCentral Lite product, read the following:

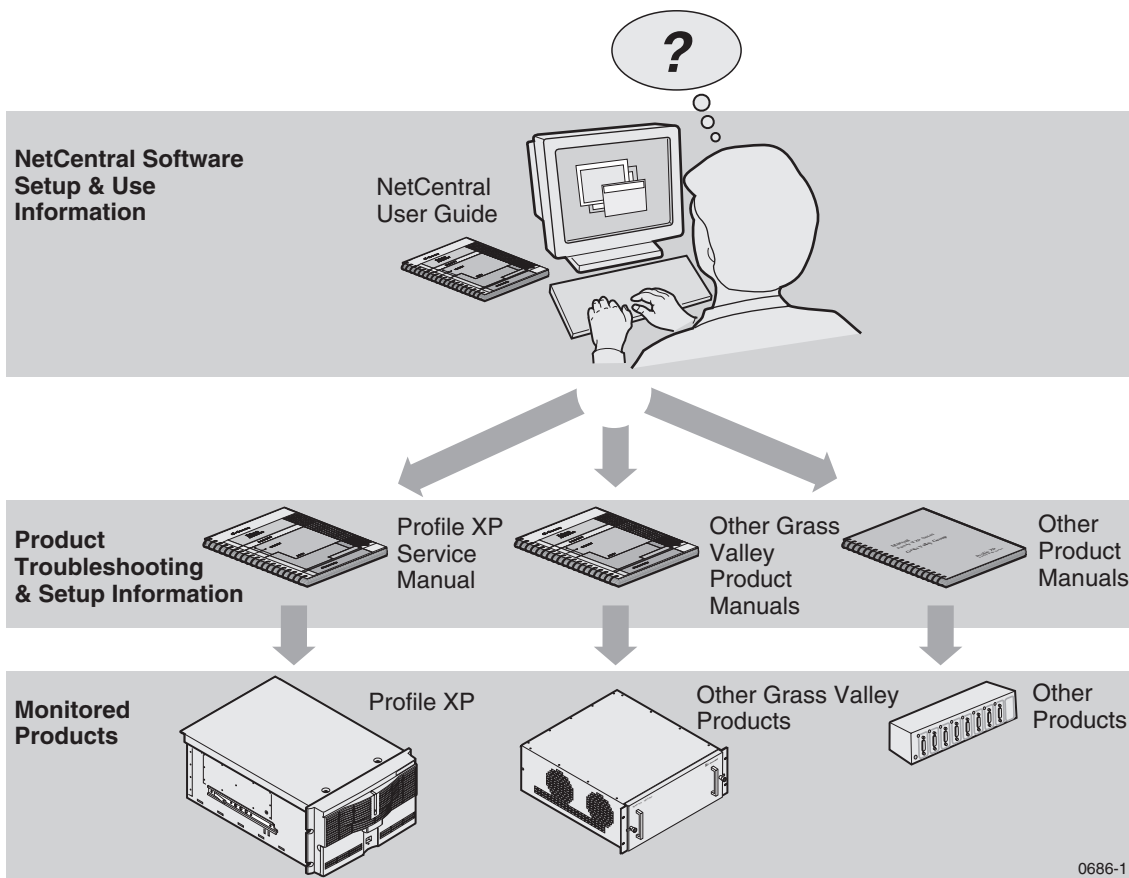
- [“About documentation for NetCentral Lite” on page 12](#)

For all NetCentral products, also read the following:

- [“Grass Valley Product Support” on page 13](#)

About documentation for the NetCentral system

In the same way that the NetCentral system monitors multiple types of products, so the information about the NetCentral system is distributed across multiple manuals. This manual, the NetCentral User Guide, contains explanations and instructions for getting the NetCentral manager software installed, configured, and operating correctly so that it can monitor your devices. Manuals that come with each type of monitored device contain descriptions of any additional software that must be installed, as well as the messages, logs, applications, and features that are specific to that type of device. Therefore, to ensure that you have all the information necessary to install and use the complete NetCentral system, you need this NetCentral User Guide and the manuals for each type of product monitored, as illustrated by the following diagram



Using this manual

This NetCentral User Guide is organized around the tasks necessary for implementing the NetCentral system and optimizing its use for your particular environment.

For understanding the NetCentral system, read the following sections:

- This *Preface* explains how information is distributed across manuals for products that make up the NetCentral system.
- [Chapter 1, Overview of the NetCentral system](#) — Describes the NetCentral system as a whole, including core technologies and how they are used.

For installation and basic setup of the NetCentral system, read the following section:

- [Chapter 2, Installing the NetCentral system](#) — Describes the requirements and procedures necessary to get a basic NetCentral system installed and working.

For operating the NetCentral system to monitor your devices, read the following sections:

- [Chapter 3, Monitoring with the NetCentral system](#) — Explains how NetCentral monitors devices for you and how you can use NetCentral to check detailed device information.
- [Chapter 4, Managing messages and actions](#) — Describes how you can configure the NetCentral system to present, distribute, and deliver device information to suit the policies and system environment of your facility.

For administering the NetCentral system, read the following sections:

- [Chapter 5, Administering the NetCentral system](#) — Explains how to control operation, restrict access, and protect the NetCentral system.
- [Chapter 6, Troubleshooting the NetCentral system](#) — Explains how to solve common problems with the NetCentral system.

For advanced customization of the NetCentral system, read the following section:

- [Appendix A, Graphical view tutorial](#) — Provides detailed procedures for creating an detailed Graphical view of a typical system. Read this section for examples of how you can apply these features to your own system.

About documentation for NetCentral Lite

NetCentral Lite is a version of NetCentral that is bundled with Profile system software. It comes pre-installed on your new Profile XP Media Platform. The functionality of NetCentral Lite is limited to the Profile XP Media Platform, as follows:

- Each Profile XP acts as its own NetCentral monitoring station.
- The NetCentral Lite manager software on the Profile XP is capable of monitoring the local Profile XP and its attached RAID storage devices only
- Auto-discovery works only for the local Profile XP and its storage devices.
- You may not remove the local Profile XP from the NetCentral Lite interface
- Only the following actions are enabled:
 - Beep
 - Flash LED
 - Trigger Profile XP GPI

For installing NetCentral Lite, read your *Profile XP Release Notes*.

For documentation on using NetCentral Lite, access the Help File on the NetCentral Lite Help menu.

NetCentral Lite corresponds to 3.x versions of NetCentral manager, so while its functionality is similar, its interface is significantly different than the 4.x version of NetCentral manager documented in this manual.

Grass Valley Product Support

To get technical assistance, check on the status of problems, or report new problems, contact Grass Valley Product Support via e-mail, the Web, or by phone or fax.

Web Technical Support

To access support information on the Web, visit the product support Web page on the Grass Valley Web site. You can download software or find solutions to problems by searching our Frequently Asked Questions (FAQ) database.

World Wide Web: <http://www.thomsongrassvalley.com/support/>

Technical Support E-mail Address: gvtechsupport@thomson.net

Phone Support

Use the following information to contact product support by phone during business hours. Afterhours phone support is available for warranty and contract customers.

United States	(800) 547-8949 (Toll Free)	France	+33 (1) 34 20 77 77
Latin America	(800) 547-8949 (Toll Free)	Germany	+49 6155 870 606
Eastern Europe	+49 6155 870 606	Greece	+33 (1) 34 20 77 77
Southern Europe	+33 (1) 34 20 77 77	Hong Kong	+852 2531 3058
Middle East	+33 (1) 34 20 77 77	Italy	+39 06 8720351
Australia	+61 3 9721 3737	Netherlands	+31 35 6238421
Belgium	+32 2 3349031	Poland	+49 6155 870 606
Brazil	+55 11 5509 3440	Russia	+49 6155 870 606
Canada	(800) 547-8949 (Toll Free)	Singapore	+656379 1390
China	+86 106615 9450	Spain	+ 34 91 512 03 50
Denmark	+45 45968800	Sweden	+46 87680705
Dubai	+ 971 4 299 64 40	Switzerland	+41 (1) 487 80 02
Finland	+35 9 68284600	UK	+44 870 903 2022

Authorized Support Representative

A local authorized support representative may be available in your country. To locate the support representative for your country, visit the product support Web page on the Thomson Grass Valley Web site.

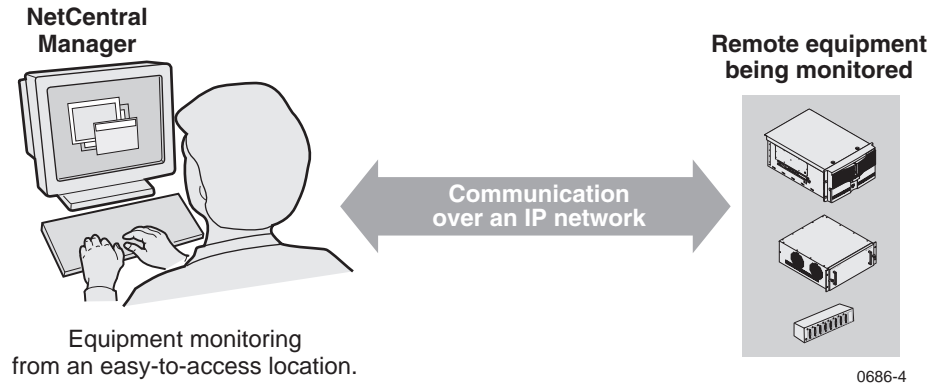
Overview of the NetCentral system

This section contains the following topics:

- [“System summary” on page 16](#)
- [“What NetCentral does” on page 17](#)
- [“How NetCentral works” on page 18](#)
- [“Technologies NetCentral uses” on page 20](#)

System summary

The NetCentral system is a suite of software modules that work together to monitor and report the operational status of your facility's equipment from one or more computers. The NetCentral system runs in a Microsoft Windows desktop environment and uses Simple Network Management Protocol (SNMP), Syslog, and other industry standard technologies to communicate over an Internet Protocol (IP) network with Grass Valley and partner products, as illustrated by the following diagram:



The NetCentral system gives facility engineers and equipment operators the ability to do the following:

- Be continuously aware of the moment-by-moment status of multiple devices
- Identify problems before they become critical
- Understand why a device is malfunctioning
- Consider recommendations for corrective action
- Research messages and logs for information about previous status changes
- Check status and troubleshoot from a remote location

The NetCentral system provides a well-developed set of features designed specifically for the TV and video industry. This allows you to concentrate on the management of your equipment while minimizing network management overhead.

Grass Valley SNMP MIBS are written in SMIV2 (Structure of Management Information). All Grass Valley agents support SNMPv1. SNMPv2c is supported by specific operating systems, such as Windows 2000 or Windows XP. NetCentral manager accepts messages from either SNMPv1 or SNMPv2c agents.

Check your *NetCentral Release Notes* for information about new features and for the latest list of device-types that NetCentral monitors.

What NetCentral does

The NetCentral system automatically monitors your equipment 24 hours a day, seven days a week. In this automatic mode, the NetCentral system does the following:

- Periodically checks devices to see if they are still in contact with the NetCentral server
- Indicates status levels for devices and their subsystems with easy-to-understand icons
- Receives and displays messages from monitored devices that explain status conditions and suggest corrective actions
- Captures all status messages in a database for later retrieval and analysis
- Notifies you of status conditions, based on rules that you define

You can also manually check your equipment for specific status information at any time with the NetCentral system interface. When you use the NetCentral system manually, you can do the following:

- See at a glance the overall status of multi-device systems, devices by location, or other arrangements to represent your system environment
- View details of current status conditions for individual devices and their subsystems
- Search messages and logs for all previous status conditions
- Troubleshoot your equipment
- Monitor from a PC connected to the internet from anywhere in the world

How NetCentral works

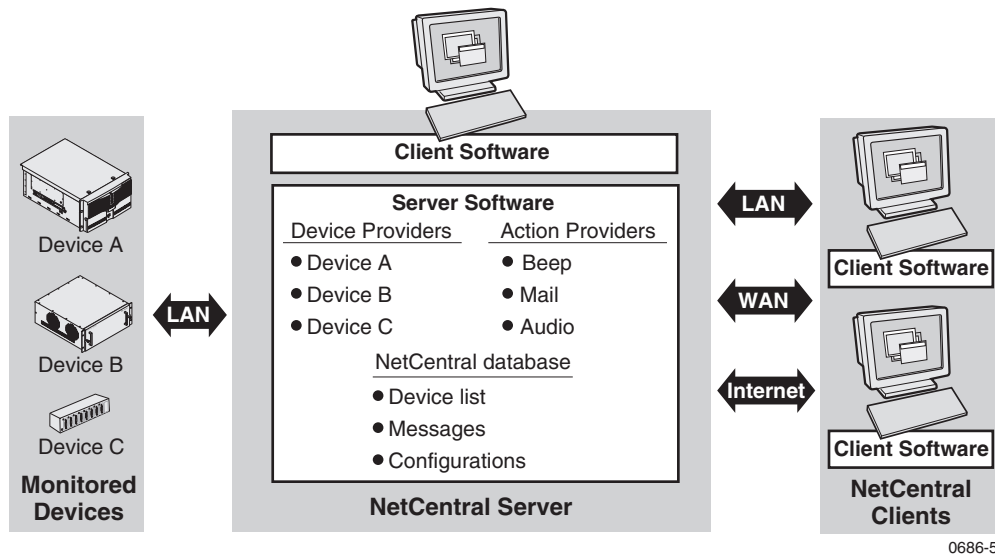
The following sections explain how SNMP monitoring with the NetCentral system works by describing its main parts and relating narratives of how messages and functionality flow in typical use.

- [“Architecture of NetCentral” on page 18](#)
- [“Components of NetCentral” on page 19](#)

For information about Syslog monitoring refer to [“Monitoring with multiple protocols” on page 42](#).

See also [Appendix C, Examples of typical NetCentral systems](#).

Architecture of NetCentral



NetCentral software has a client/server architecture. The server software includes the SNMP manager and carries the primary functionality of the NetCentral system, while the client software functions as a NetCentral viewer and allows the interface to run on PCs via a local connection, a network, or the Internet. You can connect from multiple clients to a single server. Connecting from a single client to multiple servers is not supported.

NetCentral integrates with each type of device through a software component called a device provider. When you check a specific status condition on a device, NetCentral communicates through the device provider with the device and displays the status condition in the interface. If a device experiences a change in status, the device sends a message to NetCentral. The server software pushes status indicators to its clients, enters the change in the NetCentral log, and triggers any actions that you have configured. The server software controls these actions, such as sounding audible alerts or sending e-mail, through software components called action providers. The NetCentral database stores records of messages, actions fired, custom configurations, and devices monitored.

Components of NetCentral

The NetCentral software suite has several components which exist as files on the NetCentral server. NetCentral functionality is distributed among these components, which work together as described in the following sections.

- [“NetCentral core software”](#)
- [“Device providers”](#)
- [“Action providers”](#)
- [“HTML files with active drawings”](#)

NetCentral core software

This is the central software component with which all other components interact to make a working system. It supports multiple protocols, such as Simple Network Management Protocol (SNMP) and Syslog. The core software incorporates the SNMP manager that performs the primary centralized monitoring functions. It also provides software interfaces for plugging in devices and actions.

This software is installed on the NetCentral server. The default location for software components on the server is in *C:\Program Files\Thomson Grass Valley\NetCentral\bin*. The core software runs as Windows services. Refer to [“Verifying components installed and running” on page 118](#).

Device providers

A device provider is a software component that plugs into the core software. The device provider acts as a window through which the core NetCentral software “sees” a device and propagates that view into the user interface. Each type of device has its own provider. All devices of a particular type interact with the core NetCentral software through their provider.

Device providers reside in *C:\Program Files\Thomson Grass Valley\NetCentral\DeviceProviders*. Some examples of device provider file names are *ProfileXpProvider.dll* and *ModularProvider.dll*.

Action providers

An action provider is a software component that plugs into the core software. The action provider directs the PC as it carries out an action. Each type of action has its own provider. All actions of a particular type interact with the core NetCentral software through their provider.

Action providers reside in the same directory as the core NetCentral software. Some examples of action provider file names are *Beep.dll* and *PlayAudio.dll*.

HTML files with active drawings

NetCentral’s Graphical view displays images and HTML pages. These pages are overlaid by an annotation layer that contains active drawings.

Images are provided at *C:\Program Files\Thomson Grass Valley\NetCentral\bin\imagelibrary*

Technologies NetCentral uses

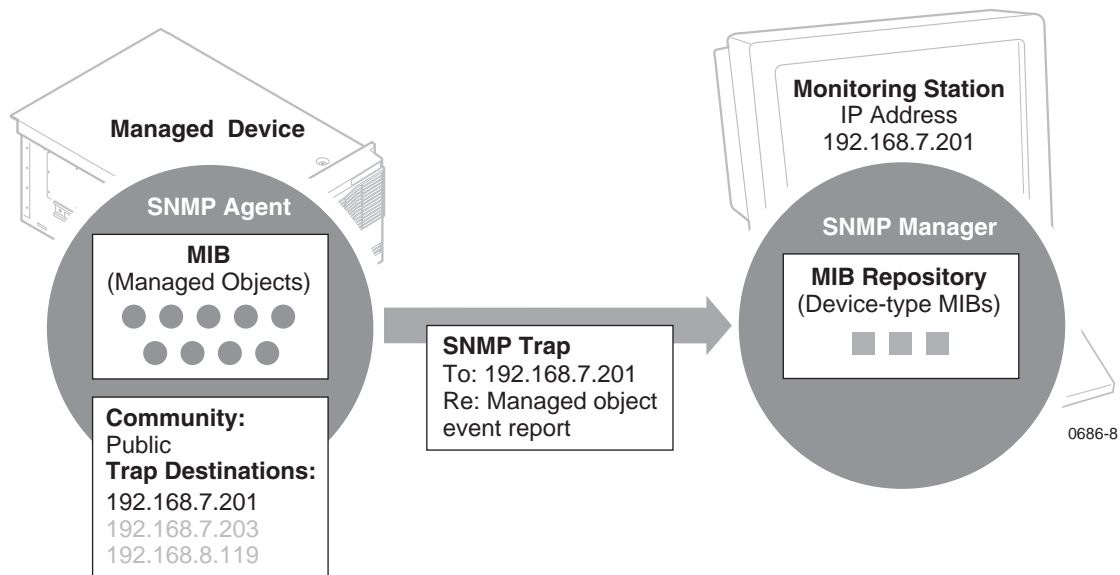
The NetCentral system uses industry standard technologies, tailored to meet the unique needs of the TV and video industry. This makes the NetCentral system open and adaptable for a wide range of applications. The following sections explain these technologies and how the NetCentral system uses them.

- [“Simple Network Management Protocol” on page 21](#)
- [“Syslog” on page 22](#)
- [“.Net” on page 22](#)
- [“FTP” on page 22](#)
- [“SQL” on page 22](#)
- [“XML” on page 23](#)
- [“Hypertext Markup Language” on page 23](#)
- [“Active drawings” on page 23](#)

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their function, as defined by the Internet Engineering Task Force (IETF). SNMP is designed as a connectionless, application-layer protocol that facilitates the exchange of management information between networked devices. SNMP can be used on diverse systems, such as computer data networks, heating and cooling control networks, and irrigation networks. NetCentral uses SNMP for the efficient remote monitoring of video and other media-related equipment.

A simplified view of how SNMP works in the NetCentral system to send SNMP trap messages is illustrated in the following diagram:



A **SNMP-managed device** is a network device that contains a SNMP agent and resides on a managed network. Managed devices collect and store management information (such as disk errors, temperature, video and audio status) and make this available to network management stations using the SNMP protocol. A QLogic Fibre Channel switch is an example of an SNMP-managed device.

A **SNMP agent** is a software module that resides on a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. For example, the Network Interface Module on a 8900 Modular frame contains a SNMP agent.

The **SNMP manager** is an application that monitors managed devices. One or more managers may exist in a network and monitor any of the managed devices. The NetCentral software that runs on the NetCentral server PC is primarily a SNMP manager, but with a specific design and added functionality for the TV and video industry.

A **management information base (MIB)** is a collection of managed objects (variables) that are properties of a device and are organized hierarchically. The agent maintains the MIB. The manager contains a repository of the MIBs from each type of

managed agent. The IETF has standardized MIBs for different classes of device like printers, routers, etc. Proprietary extensions are also allowed. For example, a Profile XP Media Platform, an 8900 Modular frame, and a QLogic Fibre Channel switch each have their own MIB.

Traps enable an agent to notify the management station of significant events such as errors on the device. SNMP trap messages are sent unsolicited on the network. Trap destinations are configured on the device so that traps are sent to one or more management stations. For example, when the disks on a Profile XP Media Platform approach maximum capacity, the Profile XP Media Platform sends out a trap that the management station interprets and displays as the “Storage Capacity Depletion” message.

Grass Valley MIBs are written in SMIV2 (Structure of Management Information). All Grass Valley agents support SNMPv1. SNMPv2c is supported by specific operating systems, such as Windows 2000 or Windows XP. NetCentral manager accepts messages from either SNMPv1 or SNMPv2c agents.

A **SNMP community** identifies a collection of SNMP managers and agents. The use of a community name provides primitive security and context checking for both agents and managers that receive requests and initiate trap operations. For example, an agent won't accept a request from a manager outside the community. In a typical NetCentral system the “public” community is used.

Syslog

While the NetCentral system's primary protocol is SNMP, it's architecture also supports communication with devices via other protocols. One of these other protocols is Syslog. Syslog protocol provides a mechanism to send event notification messages across IP networks to event message collectors - also known as syslog servers. Syslog messages are sent using UDP as its underlying transport layer mechanism to the UDP port 512.

Also refer to [“Monitoring with multiple protocols” on page 42](#).

.Net

.NET is Microsoft's XML Web services platform. It supports a client/server architecture using Web protocols so that applications perform equally well and are secure whether they communicate over a network or over the Internet. The NetCentral system's interface and client/server architecture uses .Net technology.

FTP

File Transfer Protocol (RFC-959 & 1354) is used to retrieve files (such as text log files) from devices.

SQL

NetCentral uses a Structured Query Language (SQL) based database to provide scalable access to notifications, user data, and device specific information.

XML

NetCentral uses XML (Extensible Markup Language) to store and access MIB information, as well as active drawing components.

Hypertext Markup Language

Hypertext Markup Language (HTML) is the set of “markup” codes inserted into the text of a file intended for display in a Web browser, such as Microsoft Internet Explorer. This file, when rendered by the browser, is referred to as a Web page. The individual markup codes, or tags, are interpreted by the Web browser as instructions for displaying words and images. The Graphical view uses HTML pages.

Active drawings

Active drawing technology has been developed especially for use in NetCentral. It provides the active drawing features for the HTML pages in the Graphical view. Active drawing controls allow you to copy, paste, modify, and arrange devices on the HTML page. The Active drawing controls are in this way embedded in the HTML page and make the page “come alive”, in that the drawings can actively depict the current state of your monitored devices and immediately show any status changes that occur.

Installing the NetCentral system

This section contains the instructions for getting the NetCentral system installed and working on your network. Topics included are as follows:

- [“Preparing for installation” on page 25](#)
- [“Installing software” on page 31](#)
- [“Getting started” on page 36](#)

For overview diagrams of example NetCentral systems, see [Appendix C, *Examples of typical NetCentral systems* on page 161](#).

Preparing for installation

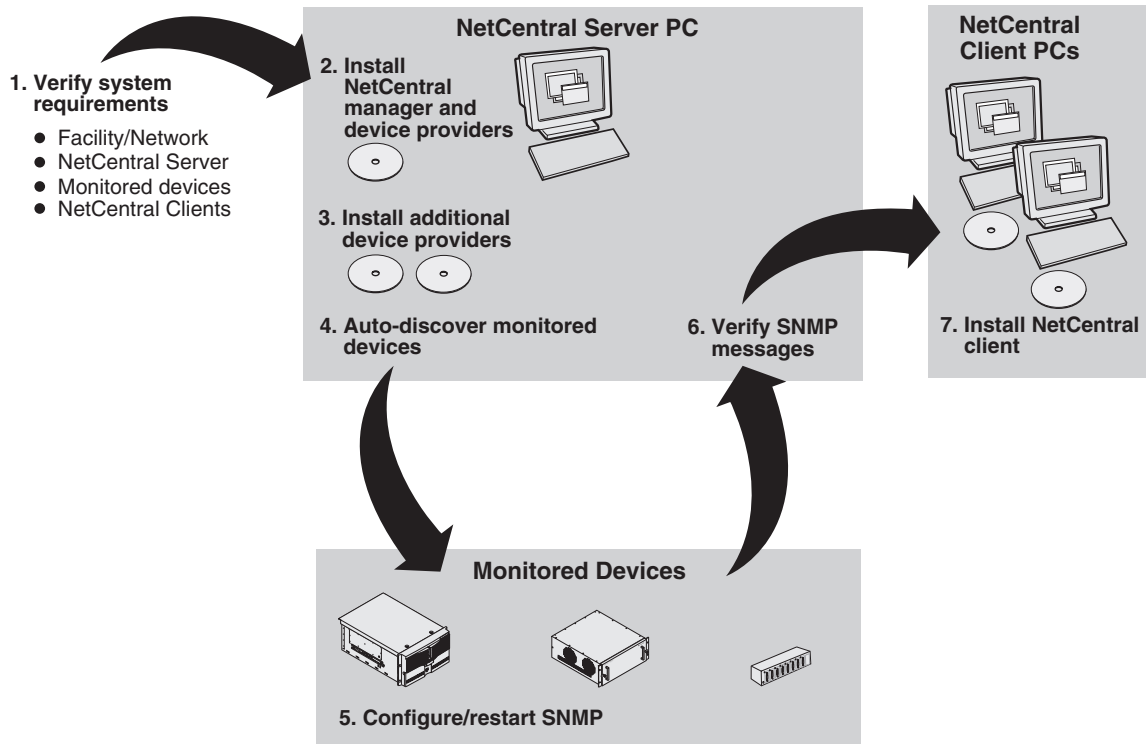
Before you install any software, read through the following topics to familiarize yourself with the overall install process and to ensure that you have the necessary systems in place to support your NetCentral installation.

- [“Installation overview” on page 26](#)
- [“Installation checklist” on page 27](#)
- [“Facility requirements” on page 28](#)
- [“NetCentral server requirements” on page 28](#)
- [“NetCentral client requirements” on page 29](#)
- [“Monitored device requirements” on page 30](#)
- [“Verify and record network settings” on page 30](#)

NOTE: *These procedures require that you be logged in to Windows as administrator or as a user with administrator-level privileges.*

Installation overview

The following diagram provides a summary of tasks.



For detailed steps refer to the “[Installation checklist](#)” in the next section.

Installation checklist

The following checklist guides you through installation and setup tasks. Use the specified documentation sources to ensure you are doing each task correctly.

	Accomplish these tasks on the NetCentral server PC...	And these tasks on monitored devices...	And these tasks on NetCentral client PCs...	Using this documentation.
<input type="checkbox"/>	Verify system requirements. If necessary, install SNMP, SQL, IIS, Acrobat Reader	Verify system requirements. On some devices you might have to unlock, install, or otherwise prepare the SNMP agent on the device.	Verify system requirements	“Facility requirements” on page 28 “NetCentral server requirements” on page 28 “NetCentral client requirements” on page 29 “Monitored device requirements” on page 30
<input type="checkbox"/>	Verify/record network settings	Verify/record network settings	Verify/record network settings	“Verify and record network settings” on page 30
<input type="checkbox"/>	Install NetCentral server software and included device providers as applicable. A restart might be required.	—	—	“Installing NetCentral software on the server” on page 31
<input type="checkbox"/>	If not installed with server software, install device providers for other types of monitored device	—	—	“Installing device provider software” on page 33 and your device-specific documentation
<input type="checkbox"/>	Start up NetCentral manager and auto-discover devices	—	—	“Auto-discovering devices” on page 37
<input type="checkbox"/>	For each device added, evaluate if it is sending its SNMP trap messages to the NetCentral server.	—	—	“Verify SNMP trap messages from monitored devices” on page 38 and your device-specific documentation
<input type="checkbox"/>	—	Do tasks to enable SNMP trap messages, such as configuring and/or restarting SNMP.	—	“Restart SNMP services on monitored devices” on page 38 and your device-specific documentation
<input type="checkbox"/>	Evaluate the list of added devices and, if necessary, add and/or remove devices.	—	—	“Adding and removing devices” on page 40
<input type="checkbox"/>	Verify devices and read additional instructions, if any.	Do remaining tasks, if any, until all devices are added and fully monitored.	—	“Accomplish other device-specific preparations” on page 42 and your device-specific documentation
<input type="checkbox"/>	—	—	Install client software	“Installing NetCentral software on clients” on page 32
<input type="checkbox"/>	If monitoring via Syslog, add devices	Configure Syslog targets	—	“Monitoring with multiple protocols” on page 42 and your device-specific documentation

As you work through these steps, make sure that you restart the NetCentral server and the monitored devices or their services as directed. Since the NetCentral system works through several layers of standard technologies and protocols, these restarts complete the installation and registration of each layer and provide the foundation for the installations at the next layer.

To help you understand the standard Windows procedures for some of these steps, refer to [Appendix D, Examples of Windows procedures](#).

Facility requirements

Your facility should provide the following to support the complete NetCentral system:

- A single NetCentral server PC. The NetCentral system does not support multiple servers.
- One or more monitored devices
- Optional: One or more NetCentral client PCs
- An IP network connecting all of the above.
- If using E-mail for notifications, your NetCentral system needs access to your facility's E-mail server.
- If one or more NetCentral clients are outside your secure network, you will need security components, such as a firewall, capable of providing secure access.

NetCentral server requirements

- Microsoft Windows XP Professional U.S. version (Click **Start | Settings | Control Panel | Regional Options** to verify U.S. version)
-or-
Microsoft Windows 2000 Professional U.S. version with Service Pack 4 or higher
- Pentium III or higher class processor, 2 GHz or greater
- 1 GB RAM
- 400 MB hard disk space
- Static IP address recommended. Refer to [“About the IP address of a NetCentral server” on page 29](#). You can also optionally assign a name to the server.
- IP Network connection, typically over an Ethernet adapter for LAN environments
- Network access to all monitored devices and NetCentral clients
- Internet Explorer version 6 or higher
- Internet Information Server 4.0 (IIS) or higher. Install from **Start | Settings | Control Panel | Add/Remove Programs | Add/Remove Windows Components**.
- SNMP services installed. Install from **Start | Settings | Control Panel | Add/Remove Programs | Add/Remove Windows Components | Management and Monitoring Tools**.
- SNMP community name. The default setting is “public”, which is all that is necessary for most NetCentral systems.

- Microsoft SQL Server Desktop Engine Version 8.00.194 or higher. The installation program is provided on the NetCentral Manager CD.
- Adobe Acrobat Reader version 6 or higher. The installation program is provided on the NetCentral Manager CD.
- Sound card and speakers, if playing audio files as a notification

Refer to [“Verifying components installed and running” on page 118](#).

These requirements assume that the PC is dedicated to its use as a NetCentral server and that it is not sharing significant system resources with other applications.

About the IP address of a NetCentral server

For the most reliable monitoring, use a static IP addresses for your NetCentral server. Your server’s Internet Protocol (IP) address is key to its ability to receive the SNMP traps that carry NetCentral system messages. In some network environments, such as those using Dynamic Host Configuration Protocol (DHCP), IP addresses are assigned dynamically, which means that under certain conditions your server could be assigned a new IP address without your knowledge. If the IP address changes, the server will cease to receive SNMP traps, which means it will no longer indicate status changes from devices or trigger actions for notification. If your server has a dynamic IP address, contact your network administrator to determine if it is persistent enough to give you the monitoring reliability you require.

With the following procedure you can learn your server’s IP address and determine whether it is static or dynamic.

1. From the Windows taskbar on the server, click **Start | Programs | Command Prompt**. The Command Prompt window appears.
2. At the command prompt, type the following:

```
ipconfig /all
```

Press Enter to display the IP configuration information

3. Check for “Lease Obtained” and “Lease Expires” lines. If these lines are not present, your server has a static IP address. If these lines are present, your server has a dynamic IP address. Typically, the mechanisms on the network that assign dynamic IP address, such as a DHCP server, will re-assign the same IP address to a PC when its lease expires. If the dates indicate that the lease for your IP address expires periodically, you should check with your network administrator to determine the conditions under which your server could be assigned a different IP address.

NetCentral client requirements

- Microsoft Windows XP Professional (U.S. version)
-or-
Microsoft Windows 2000 Professional (U.S. version) with Service Pack 4 or higher
- Pentium III or higher class processor, 1 GHz or greater
- 512 MB RAM

- 100 MB hard disk space
- IP address. You can also optionally assign a name to the client.
- IP Network connection, typically over an Ethernet adapter for LAN environments.
- Internet Explorer version 6 or higher
- Adobe Acrobat Reader version 6 or higher. The installation program is provided on the NetCentral Client CD.
- Network or Internet access to the NetCentral server
- Sound card and speakers, if playing audio files as a notification

Monitored device requirements

NetCentral monitors a wide range of device-types. Some types have unique requirements for NetCentral monitoring that are beyond the scope of this *User Guide*. Refer to the documentation for each device-type for these special requirements. However, all monitored devices have some requirements in common, as follows:

- SNMP agent — All devices supported for monitoring by the NetCentral system have an SNMP agent. On most devices the agent software is embedded and no installation is required. However, on some devices you must update or “unlock” SNMP agent software. On some devices you must install a board on which the SNMP agent software is embedded. Read the documentation for the device and do installations or upgrades as instructed.
- SNMP community name — The default setting is “public”, which is all that is necessary for most NetCentral systems. Refer to your device-specific documentation for procedures to verify and set the SNMP community.
- Device provider — You must have a NetCentral device provider for each device-type you monitor. The device provider is installed on the NetCentral server PC, not the monitored device. It is required to enable that device-type’s monitoring with NetCentral.
- IP address. You can also optionally assign a name to the device, if applicable.
- IP Network connection, typically over an Ethernet adapter for LAN environments
- Network access to the NetCentral server PC

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 42](#).

When you install the device provider on the NetCentral server PC, the device provider installation program provides online documentation that explains the specific requirements for monitoring that device-type with the NetCentral system.

Verify and record network settings

Make sure that you know the following information for the NetCentral server, each monitored device, and each NetCentral client:

- IP address
- Machine name (if applicable)

Write down this information, as you will need it for subsequent procedures.

Installing software

The following topics provide procedures for installing NetCentral software components:

- [“Installing NetCentral software on the server” on page 31](#)
- [“Installing NetCentral software on clients” on page 32](#)
- [“Reinstalling NetCentral software” on page 33](#)
- [“Uninstalling NetCentral software” on page 33](#)
- [“Installing device provider software” on page 33](#)
- [“Uninstalling device provider software” on page 35](#)

Installing NetCentral software on the server

Install the NetCentral server software on the NetCentral server PC. Make sure that SQL is installed and the PC has been restarted at least once since it was installed, as the NetCentral server installation program aborts if it does not detect SQL. Refer to [“NetCentral server requirements” on page 28](#) and [“Verifying components installed and running” on page 118](#).

The NetCentral server installation program installs the following:

- NetCentral server components
- NetCentral client components
- Microsoft .NET, if it is not already installed.

The NetCentral server installation process also incorporates the installation program for NetCentral device providers. Device provider availability varies depending on product design and licensing. Some device providers are readily available as part of the NetCentral server installation process. Others require specific CDs, setup files, or license keys.

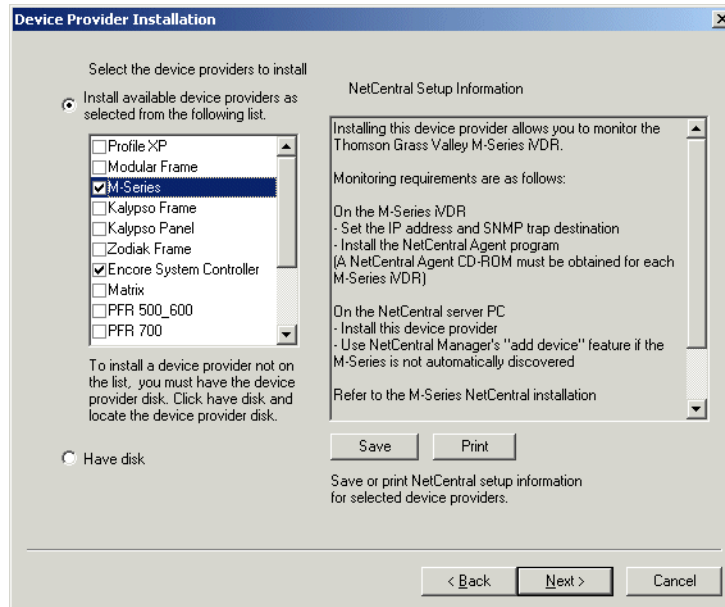
NOTE: The following procedures require that you be logged in to Windows as administrator or as a user with administrator-level privileges.

To install NetCentral server software, do the following:

1. Close all Windows programs.
2. Locate and open the NetCentral server installation file. It is called *ServerSetup.exe*. You can find this file on the *NetCentral Manager* CD-ROM. The installation wizard opens.
3. Read the setup screens, clicking the **Next** button to move through the installation process.
4. If .Net is not already installed on the PC, the installation program prompts you to install it. Confirm the installation and complete the .Net install wizard.
5. Click **Next** and **Finish** to complete the installation of server software.
6. When prompted “Do you want to install Device Providers now?”, click **Yes**. The

device provider installation program opens.

7. Click next until you arrive at the screen that lists the device providers available for installation.



8. Select the device providers for which you are licensed. From this screen you can view a short explanation of the requirements for monitoring each listed device type. If a device provider that you need is not listed, it must be procured from Thomson Grass Valley and installed as in [“Installing device provider software” on page 33](#).
9. Click the **Next** button to move through the remaining screens and complete the installation wizard. If prompted to restart, you must do so. Click **Yes** and **Finish**.
10. If you also received a NetCentral Service Pack, install it now to bring your software up to date with the latest improvements.

Installing NetCentral software on clients

You can operate the NetCentral system entirely from the local NetCentral server PC, so additional client PCs are not required. However, you can purchase client licenses for LAN connected or Web connected PCs. This allows you to operate the NetCentral system remotely from these PCs as well.

Install the NetCentral client software on each of your NetCentral clients. This installs the following components:

- NetCentral client components.
- Microsoft .NET, if it is not already installed.

Before installing NetCentral software on client PCs, make sure NetCentral services are running (the NetCentral interface is started) on the NetCentral server PC.

NOTE: The following procedures require that you be logged in to Windows as administrator or as a user with administrator-level privileges.

To install NetCentral client software, do the following:

1. On the NetCentral client PC, close all Windows programs.
2. Locate and open the NetCentral client installation file. It is called *ClientSetup.exe*. You can find this file on the *NetCentral Client* CD-ROM. The installation wizard opens.
3. Read the setup screens, clicking the **Next** button to move through the installation process.
4. If .Net is not already installed on the PC, the installation program prompts you to install it. Confirm the installation and work through the .Net install wizard.
5. When you arrive at the screen that asks for the NetCentral server IP address, enter the IP address of the NetCentral server. Do not enter multiple NetCentral servers. The NetCentral system does not support access to multiple NetCentral servers from a single NetCentral client.
6. Click the **Next** button to move through the remaining screens and complete the installation wizard. If prompted to restart, you must do so. Click **Yes** and **Finish**.
7. If you also received a NetCentral Service Pack, install it now to bring your software up to date with the latest improvements.

Reinstalling NetCentral software

Similar to the procedures for installing NetCentral server and client software, you can open the NetCentral installation program and use the installation wizard to reinstall the software.

Uninstalling NetCentral software

Use the standard procedures for the machine's operating system to uninstall NetCentral software. When you do so, take the following points into consideration:

- Uninstalling server software — This removes all NetCentral components and data from the machine. This includes the NetCentral database, which contains all logs, messages, records of devices added, and custom configurations. If you want to recover any of this information you should first backup the NetCentral database, as described by [“Backing up the NetCentral database” on page 117](#).
- Uninstalling client software — You can remove software on NetCentral clients without affecting the NetCentral database. The database remains intact on the server and all configurations and data are available when the client software is reinstalled. However, you might have to restore on the client PC any HTML files and referenced images or other files associated with graphic views or actions that you have configured.

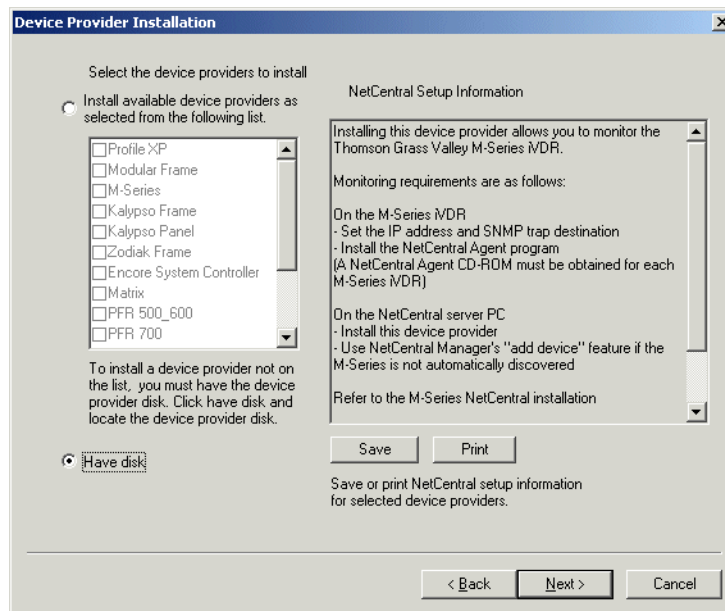
Installing device provider software

The NetCentral server installation process copies device provider files onto the PC and opens the device provider installation program in which you can select device providers to install. If all the device providers for which you are licensed have been

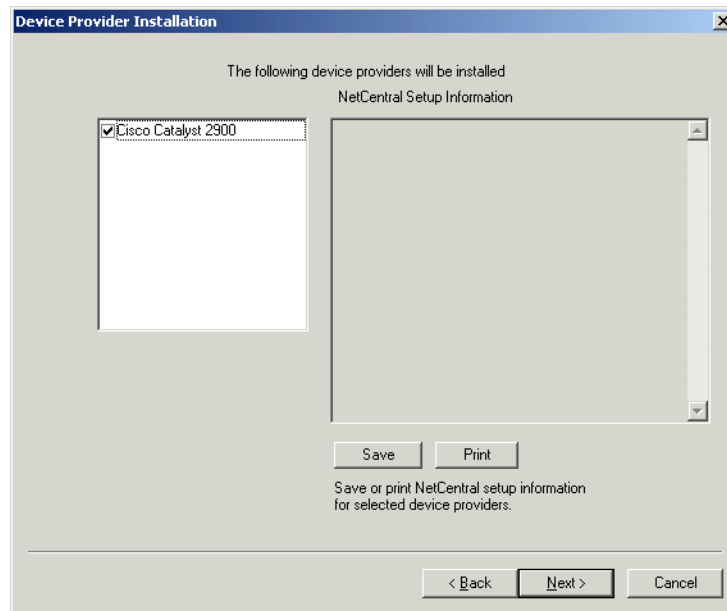
copied onto the NetCentral server PC, you can install them as part of the NetCentral server installation process, as explained in [“Installing NetCentral software on the server” on page 31](#), or you can install them later using the following procedure.

However, not all device providers are copied onto the NetCentral server PC as part of the NetCentral server installation process. Depending on product ownership and licensing, you might have to procure the device providers on a CD or via other distribution mechanisms. Once you have procured the device provider installation files and inserted the CD or otherwise made the files accessible to the NetCentral server PC, install device providers as follows:

1. Make sure you are logged on to NetCentral with administrator-level privileges.
2. Click **File | Add | Device Provider**. The device provider installation program opens.
3. Agree to the license agreement and click **Next** until you arrive at the screen that lists the device providers available for installation.
4. If one or more of the device providers you need are listed, it means those device provider files have already been copied onto the NetCentral server PC. Select one or more device providers and then continue with step 6 of this procedure.
5. If a device provider you need is not listed, do the following:
 - a. Click **Have Disk**.



- b. Click **Next**. The Select dialog box opens.
- c. Browse to the location of the installation files for a device provider, select the *.ncp file for the device provider, and click **Select**. The Select dialog box closes and the device provider is automatically selected in the device provider installation program.



6. Click **Next** to move through the remaining screens complete the installation wizard.

7. Repeat this procedure to install additional device providers.

Refer to the manual or installation instructions for the type of monitored device to determine the requirements for NetCentral monitoring.

If you are unsure if a device provider is correctly installed and registered, you can use the Diagnostic tool to test and verify, as explained in [“Diagnosing NetCentral problems” on page 124](#). When you are satisfied that your NetCentral server has a correctly installed NetCentral device provider for each type of device you are monitoring, continue with [“Auto-discovering devices” on page 37](#).

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 42](#).

Uninstalling device provider software

Use the standard procedures for the PC’s operating system to uninstall device provider software. When you do so, take the following points into consideration:

- **Device specific messages** — When the device provider software is uninstalled all logs and records of messages received from devices of that type are deleted from the NetCentral database.
- **Records of devices added or removed** — When the device provider software is uninstalled, all records of devices of that type that have been added or removed from the NetCentral system are lost. If the device provider software is reinstalled, devices must be again added or removed to build the same list of devices.

If you want to recover any of this information you should first backup the NetCentral database, as described by [“Backing up the NetCentral database” on page 117](#).

Getting started


Work through the following topics to create a working NetCentral system:

- [“Opening NetCentral manager for initial setup” on page 36](#)
- [“Auto-discovering devices” on page 37](#)
- [“Restart SNMP services on monitored devices” on page 38](#)
- [“Verify SNMP trap messages from monitored devices” on page 38](#)
- [“Set SNMP trap destinations on monitored devices” on page 39](#)
- [“Adding and removing devices” on page 40](#)
- [“Accomplish other device-specific preparations” on page 42](#)
- [“Monitoring with multiple protocols” on page 42](#)

Opening NetCentral manager for initial setup

Make sure that at least one device provider is installed before opening NetCentral manager on the server PC for the first time. This allows the manager software to initiate automatic setup processes to add devices. If no device providers are installed the manager software opens but remains blank and largely non-functional.

To open NetCentral manager for initial setup tasks, do the following at the NetCentral server:

1. Make sure your current Windows login to the NetCentral server PC has administrator-level privileges.
2. Add the NCadministrator group to your current Windows login user account or to a user account that you set up. In Windows 2000 you can find the necessary settings at **Start | Settings | Control Panel | Users and Passwords | Advanced | Advanced**. Refer to [“Managing NetCentral security” on page 113](#) for more information about users, groups, and NetCentral access permissions.
3. Double-click the NetCentral icon on your Windows desktop or select **Start | Programs | NetCentral | NetCentral**. A splash screen appears and displays the progress of startup processes. After a short pause, the NetCentral main window opens and the NetCentral icon  appears in the system tray of your Windows taskbar. For more information about the NetCentral interface, read [“Overview of the NetCentral main window” on page 50](#).
4. Click **File | Logon** and log on to NetCentral with the username and password for the user account to which you added the NCadministrator group.
5. Verify that you are now logged on to NetCentral with administrator privileges, as reported by the Status bar in the lower portion of the NetCentral interface window.

Refer to [“Verifying components installed and running” on page 118](#) to make sure the software is properly installed.

When you open NetCentral manager for the first time and at least one device provider is correctly installed, manager software begins the auto-discovery process, as described in the next section.

Auto-discovering devices

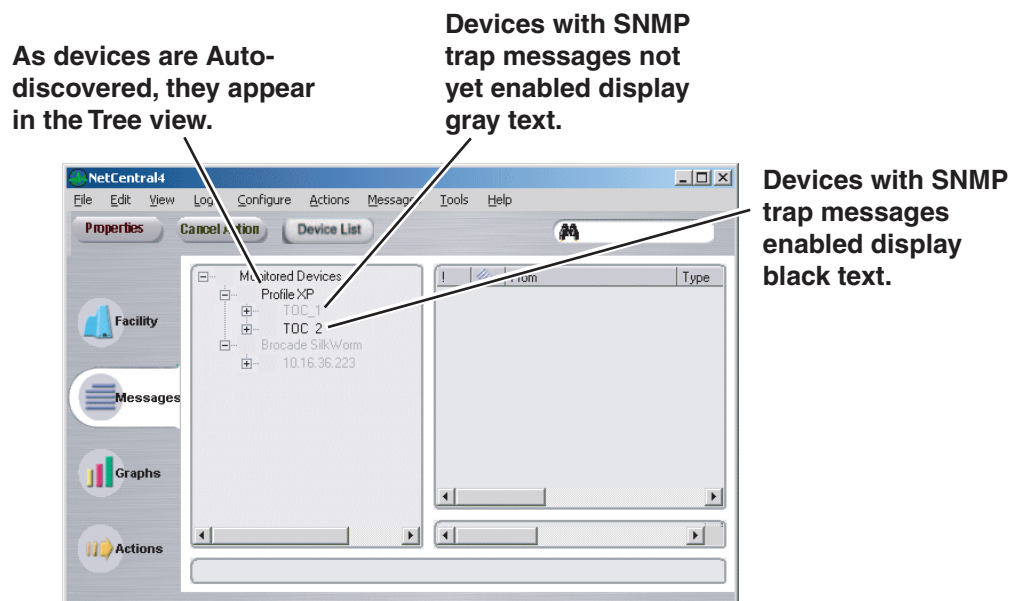
In this procedure you work with the following NetCentral automatic processes:

- The Auto-discovery process, which adds NetCentral-compatible devices
- The SNMP trap configuration process, which attempts to configure SNMP trap message destinations on devices.

A SNMP trap message is a message that comes from a device, such as the “Module mismatch” message from a 8900 Modular frame. A SNMP trap message will not find its way to the NetCentral server unless the message contains the NetCentral server’s Internet Protocol (IP) address. To embed the NetCentral server address in the message, the address must be entered on the device as a SNMP trap destination.

To work with Auto-discovery processes, do the following:

1. On the NetCentral server PC, open the NetCentral interface. Auto-discovery starts. Make sure you are logged on with administrator privileges, as explained in [“Opening NetCentral manager for initial setup” on page 36](#). If the NetCentral interface is already open, click **Configure | Start Auto Discovery** to ensure the process is started.
2. Click **Logs | Application Logs** to open the Application Logs Viewer, in which you can track NetCentral’s automatic processes.
3. Wait for devices to appear in the NetCentral Tree view through the Auto-discovery process. This process searches the local network for NetCentral supported devices and adds them automatically to the NetCentral system. The first time you run NetCentral, you might have to wait several minutes before you begin to see devices as they are automatically added.



4. Check the list of devices in the Tree view. Expand nodes as necessary. Devices that are successfully added through Auto-discovery appear in the Tree View. If no devices are listed, you must manually add devices as in [“Adding and removing devices” on page 40](#) and then repeat this procedure.

5. As devices are added, the SNMP trap configuration process attempts to configure SNMP properties on each device. This process reports its results as a tooltip that appears when you hover your cursor over a device in the Tree view. The process also reports its results in the NetCentral Application Logs Viewer. Identify messages for devices and proceed as follows:
 - If devices have a "...successfully configured SNMP..." tooltip message or a "Trap target...is set" Application Logs Viewer message, it means that NetCentral successfully entered the IP address of the NetCentral server as a SNMP trap destination on the monitored device. If at least one device has this message, proceed with the next section ["Restart SNMP services on monitored devices" on page 38](#).
 - If no devices have a "...successfully configured SNMP..." tooltip message or a "Trap target...is set" Application Logs Viewer message, you must manually configure devices as in ["Set SNMP trap destinations on monitored devices" on page 39](#) and then repeat this procedure.

Restart SNMP services on monitored devices

Do this task for the devices that have a "...successfully configured SNMP..." tooltip message or a "Trap target...is set" Application Logs Viewer message.

For most devices you must put the SNMP trap configuration changes into effect by restarting SNMP services on the device. The requirements for restarting SNMP services vary according to the type of device. On all devices you can restart SNMP services by restarting the device itself. On some devices there is a way to restart SNMP services without restarting the device itself. On some devices, such as those with Windows 2000 and XP operating systems, changes are put into effect without restarting SNMP services. Read your device-specific documentation for instructions. If you are not sure, restart the device.

As an example, on Windows NT devices, you can restart the SNMP Trap Service without restarting the device itself as follows:

1. Click **Start | Settings | Control Panel**. Open the **Services** icon.
2. Select **SNMP Trap Service**.
3. Click **Stop**.
4. Click **Start**.
5. Close dialog boxes.

For each device that has a "...successfully configured SNMP..." tooltip message or a "Trap target...is set" Application Logs Viewer message, do the necessary steps to put the SNMP configuration changes into effect, then continue with the next procedure ["Verify SNMP trap messages from monitored devices"](#).

Verify SNMP trap messages from monitored devices

Use this procedure after you have added a device, configured a device, restarted SNMP services on a device or otherwise adjusted your NetCentral system in its ability to receive SNMP trap messages from one or more monitored devices.

This procedure runs the SNMP trap configuration process. This is the same process that runs automatically when you start NetCentral manager. This process tests currently added devices to see if they are able to send their SNMP trap messages to the NetCentral server and if they are not able, attempts to configure SNMP trap destinations on devices. The process reports its results as a tooltip and in the NetCentral Application Logs Viewer. By running the SNMP trap configuration process and evaluating its results, you can identify devices that need no further configuration and determine the tasks required on devices that do need further configuration.

For an explanation of the SNMP trap configuration process and procedures for changing its default behavior, read [“Setting automatic SNMP trap configuration” on page 109](#).

To verify SNMP trap messages from monitored devices, do the following:

1. At the NetCentral server, click **Configure | Start SNMP Trap Message Configuration** to test all currently added devices. You might have to first click **Configure | Stop SNMP Trap Message Configuration** and then click **Configure | Start SNMP Trap Message Configuration**.
2. As the SNMP trap configuration process runs, check results in the NetCentral Application Logs Viewer.
3. Evaluate the appearance of your devices in the Tree view. For each device, determine its ability to send SNMP trap messages to the NetCentral server as follows:
 - A device with a full-resolution (not grayed-out) name or IP address has its SNMP trap messages fully enabled. You can confirm this by hovering your cursor over the device in the Tree view. A tooltip appears with the message “Able to receive SNMP trap messages ...”.
 - A device with a grayed-out name or IP address does not yet have its SNMP trap messages fully enabled. Repeat procedures as necessary until the device is able to send its SNMP trap messages to the NetCentral server. You might have to manually configure SNMP on the device, as explained in [“Set SNMP trap destinations on monitored devices” on page 39](#).
4. Proceed for each device as indicated. Once all devices have the tooltip “Able to receive SNMP trap messages ...” message, continue with this procedure.
5. If your tree view is complete — meaning that the list contains all the devices that you do want to monitor but does not contain any devices that you do not want to monitor — skip ahead to [“Accomplish other device-specific preparations” on page 42](#).
6. If your tree view is not yet complete, continue with [“Adding and removing devices” on page 40](#).

Set SNMP trap destinations on monitored devices

This section provides guidelines for setting SNMP trap destinations on monitored devices that do not support the remote SNMP trap configuration mechanism that the NetCentral manager software uses. These devices report a “...trap message

configuration...not supported” tooltip message or a “...configuration of trap target...not supported” Application Logs Viewer message. On these devices you must use a device-specific method to set a SNMP trap destination.

You set a SNMP trap destination by configuring SNMP properties. While each type of device has its own interface and methods for configuring SNMP properties, the underlying values that must be set are common to all devices, as explained in the following procedure.

To set SNMP trap destinations using a device-specific method, do the following:

1. **Determine the method for configuring SNMP properties.** Read the manufacturer’s documentation that you received with your device for specific procedures or read the example procedures later in this section. Some devices require that you go to the device itself and manually configure SNMP properties. Some devices allow you to configure SNMP properties remotely.

Within the device’s interface for SNMP properties, identify the settings for trap destinations. A trap destination might also be called a trap recipient or a trap target.
2. **Enter the NetCentral server as a trap destination.** Enter the following information to set the NetCentral server as a trap destination:
 - The IP address (or on some devices, the machine name) of the NetCentral server. Read [“About the IP address of a NetCentral server” on page 29](#) for more information about IP addresses.
 - The name of the SNMP community to which the NetCentral server belongs. Typically, this is set to “public” by default. If you use other SNMP community names, make sure you set trap destinations for each one. In any case, make sure you enter a community name for the device. A device with no SNMP community name cannot be monitored by the NetCentral system.
3. **Put changes into effect.** Usually this requires that the SNMP services on the device or the device itself be restarted. Read the manufacturer’s documentation that you received with your device for a specific procedure to accomplish this step.
4. **Verify with NetCentral manager.** On the NetCentral server, use the SNMP trap configuration process to test the device, as explained in [“Verify SNMP trap messages from monitored devices” on page 38](#).

When you install the device provider on the NetCentral server PC, the device provider installation program provides online documentation that explains the specific requirements for monitoring that device-type with the NetCentral system.

Refer to [Appendix D, Examples of Windows procedures](#) for examples of setting SNMP trap destinations on devices running a Windows operating system.

After you have successfully set trap destinations on your SNMP monitored devices, continue with [“Verify SNMP trap messages from monitored devices” on page 38](#).

Adding and removing devices

If NetCentral’s Auto-discovery feature in its default configuration does not automatically create the correct list of devices that you want to monitor, you can manually add and remove devices one at a time as explained in the following procedures.

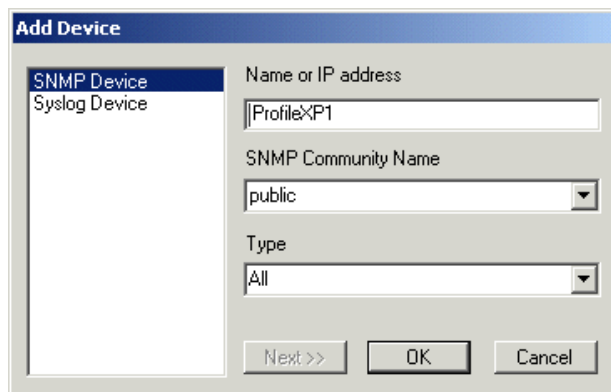
- [“Adding devices to the Tree view” on page 41](#)
- [“Removing devices from the Tree view” on page 42](#)

For related information refer to [“Adding devices” on page 104](#).

Adding devices to the Tree view

To manually add a SNMP-monitored device, do the following:

1. Make sure you are logged in to NetCentral with administrator-level privileges.
2. Click **File | Add | Device**. The Add Device dialog box opens.



3. Select **SNMP Device**.
4. Enter the name or IP address of the device you want to add.
5. Enter `public` as the SNMP community name. Refer to [“Adding devices” on page 104](#) for more information on SNMP community names.
6. To make the discovery process more efficient, on the **Type** drop-down list you can select the type of device. If the device-type you want to monitor is not on the list, it means the device provider is not installed.
7. Click the **OK** button to close the dialog box. A “Network Connection” message box appears. When the device is successfully added it appears in the Tree view.
8. Repeat this procedure until all your devices are added.
9. Evaluate the appearance and the SNMP trap configuration messages of added devices. If indicated, accomplish additional steps, as explained in [“Verify SNMP trap messages from monitored devices” on page 38](#). Once all added devices are able to send their SNMP trap messages to the NetCentral server, continue with this procedure.
10. If the only devices that are present in the NetCentral window are those that you want to monitor, skip ahead to [“Accomplish other device-specific preparations” on page 42](#).
11. If any devices are present in the NetCentral window that you do not want to monitor, continue with the next procedure [“Removing devices from the Tree view”](#).

Removing devices from the Tree view

To remove a device, do the following:

1. Make sure you are logged on to NetCentral with administrator-level privileges.
2. In the Tree view, highlight the device you want to remove.
3. Click **File | Remove**. The Delete Device message box appears, asking “Are you sure...?”.
4. Click the **Yes** button to remove the device and close the message box.
5. Repeat this procedure as necessary until all undesired devices are removed.
6. Once you have added or removed devices to create your complete tree view and all the devices listed have their SNMP trap messages enabled, continue with the next section, [“Accomplish other device-specific preparations”](#). Otherwise, repeat procedures as appropriate from earlier in this section.

Accomplish other device-specific preparations

Read the manual or installation instructions for the SNMP-monitored device and check for other installations or upgrades that are required in order to monitor the device with your NetCentral system. For example, some devices require the installation of a FTP server for the transfer of device-specific logs to the NetCentral server.

When you install the device provider on the NetCentral server PC, the device provider installation program provides online documentation that explains the specific requirements for monitoring that device-type with the NetCentral system.

If you are monitoring devices via SNMP only and each monitored device is fully functioning with all features enabled in the NetCentral system, continue with [Chapter 3, *Monitoring with the NetCentral system on page 45*](#).

If you require that some devices be monitored via Syslog, continue with the next section [“Monitoring with multiple protocols”](#).

Monitoring with multiple protocols

While the NetCentral system’s primary protocol is SNMP, it’s architecture also supports communication with devices via other protocols. One of these other protocols is Syslog. Currently the NetCentral system supports SNMP and Syslog protocols. Therefore you can monitor devices with multiple protocols as follows:

- You can monitor a device via SNMP only
- You can monitor a device via Syslog only
- You can monitor a device via both SNMP and Syslog.

How Syslog works in NetCentral

The NetCentral core software on the server PC listens for Syslog messages on UDP port 514. The NetCentral software reacts to the message as if it were a SNMP trap message, showing the message in the interface, displaying status indicators, logging the message, and triggering actions.

The Syslog protocol can have as many as eight severity levels for messages. NetCentral maps the Syslog severity levels to the appropriate NetCentral severity levels.

Setting up and using Syslog in NetCentral

Use the following steps to monitor a device via Syslog:

1. Make sure the device you want to monitor via Syslog generates Syslog messages. Check the documentation you received with the device for information about Syslog.
2. Make sure you are logged on to NetCentral with administrator-level privileges.
3. If the device is currently being monitored via SNMP and you want to now add Syslog monitoring for the device, skip ahead to step 5 of this procedure.
4. If the device is not currently being monitored, click **File | Add | Device**. The Add Device dialog box opens. Proceed as follows:
 - If you want to monitor the device via Syslog only, select **Syslog Device** and enter the IP address of the device. You can optionally enter Location information as well. Then click **OK** to save settings and close.
 - If you want to monitor the device with both SNMP and Syslog simultaneously, select **SNMP Device** and enter the IP address or name of the device. Also enter the SNMP community name (usually “public”). Then click **OK** to save settings and close.
5. On the device, configure Syslog properties so that you can enter the IP address of the NetCentral server as a Syslog target. This might be called a Syslog Daemon IP or some other term. Read the documentation you received with the device for instructions.
6. Put Syslog configuration changes into effect on the device as instructed by the documentation you received with the device.
7. Manipulate the device so that it sends a Syslog message to the NetCentral server. A Syslog-monitored device does not appear in the NetCentral interface until the NetCentral server’s first receipt of a Syslog message from the device.
8. Verify that the device appears in NetCentral as a Syslog device. Devices monitored via both Syslog and SNMP appear as SNMP devices only, yet they display both Syslog and SNMP messages.
9. Select a Syslog device and view its subsystem properties.
10. View logged Syslog messages using NetCentral message features as you would for SNMP trap messages.

When each monitored device is fully functioning with all features enabled in the NetCentral system, continue with the next section [“Monitoring with the NetCentral system”](#).

Monitoring with the NetCentral system

This section describes how the NetCentral system communicates the status of your SNMP-monitored devices.

The topics in this section are as follows:

- [“About NetCentral monitoring” on page 46](#)
- [“Accessing NetCentral” on page 47](#)
- [“Overview of the NetCentral main window” on page 50](#)
- [“Viewing information in the NetCentral main window” on page 51](#)
- [“Arranging the Tree view” on page 55](#)
- [“Creating a Facility graphical view” on page 57](#)
- [“Interpreting status indicators” on page 60](#)
- [“Responding to messages and actions” on page 63](#)
- [“Finding monitored devices” on page 66](#)
- [“Browsing device status” on page 67](#)
- [“Researching device status in NetCentral messages” on page 69](#)
- [“Exporting NetCentral messages” on page 73](#)
- [“Researching device status with graphs” on page 77](#)
- [“Researching device-specific logs” on page 79](#)
- [“Using device-specific features” on page 82](#)
- [“Viewing version information” on page 82](#)

About NetCentral monitoring

As the NetCentral system carries out its primary function as a device monitoring tool, it does most of its work automatically. In this automatic mode, the NetCentral system detects device status and notifies you of status changes in the following ways:

- NetCentral manager software periodically requests from all devices a message that confirms that they are able to communicate over the network. This is called heartbeat polling. NetCentral reports any devices that are unresponsive to the heartbeat polling. Read [“Setting heartbeat polling” on page 111](#) for more information.
- At startup NetCentral manager software triggers each device to send a test SNMP trap message. The receipt of this message at the NetCentral server confirms that the device is correctly targeting its SNMP trap messages to the NetCentral server. NetCentral reports whether devices do or do not have their messages correctly targeted. Read [“Setting automatic SNMP trap configuration” on page 109](#) for more information.
- NetCentral manager software constantly listens for the SNMP trap messages that devices send when they have a change in their status. The NetCentral system analyzes the SNMP trap messages and, based on their relative urgency, communicates to you the status information you need to keep your devices operating. Read [Chapter 4, *Managing messages and actions*](#) for more information.

If you need to troubleshoot or otherwise gather information on the health of your devices you can manually use the NetCentral system as a diagnostic tool to check both current and historical status. In this manual mode, the NetCentral system gives you the ability to do the following:

- Check the status details for any device at any time, as explained in [“Browsing device status” on page 67](#).
- Research previous status changes by viewing past messages, as explained in [“Researching device status in NetCentral messages” on page 69](#).
- Research previous status changes by viewing statistics in graph form, as explained in [“Researching device status with graphs” on page 77](#).

For Syslog monitoring, refer to [“Setting up and using Syslog in NetCentral” on page 43](#).

Accessing NetCentral

The following topics explain your options for access to the NetCentral system user interface:

- [“About access permissions” on page 47](#)
- [“Starting NetCentral” on page 47](#)
- [“Logging on and off of NetCentral” on page 48](#)
- [“Accessing NetCentral manager from a remote location” on page 48](#)
- [“Stopping NetCentral” on page 48](#)
- [“Adding NetCentral to startup” on page 49](#)

About access permissions

Any user on any NetCentral server PC or client PC can open NetCentral manager and operate the software with user-level access permissions, as explained in [“Starting NetCentral” on page 47](#). User-level access permissions are sufficient for basic device monitoring. You can view information received from devices, but features for configuring the NetCentral system are disabled.

If you need administrator-level or technician-level access permissions, you must logon to NetCentral as explained in [“Logging on and off of NetCentral” on page 48](#).

Starting NetCentral

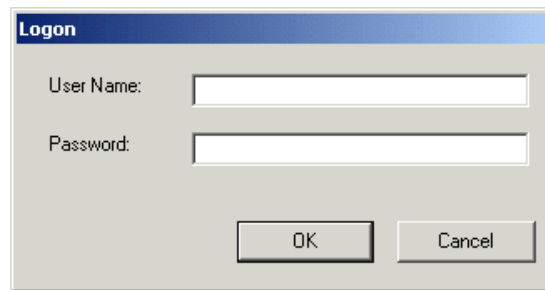
To start NetCentral, double-click the NetCentral icon on your Windows desktop or select **Start | Programs | NetCentral | NetCentral**. A splash screen appears and displays the progress of startup processes. After a short pause, the NetCentral main window opens.

If you have trouble starting NetCentral, make sure that NetCentral system components are properly installed. Refer to [Chapter 2, *Installing the NetCentral system* on page 25](#).

Logging on and off of NetCentral

The NetCentral interface always opens with user-level access permissions granted by default. Logging on to NetCentral gains technician-level or administrator-level access permissions. Logging off of NetCentral returns to user-level access permissions.

1. On the NetCentral main window, click **File | Logon**. The Logon dialog box opens.



2. Enter a user name and password that has been set up for technician-level or administrator-level access permissions.
3. Click **OK**. NetCentral manager grants appropriate access permissions, as indicated by the current logon information in the status bar at the bottom of the NetCentral window.
4. When you are ready to return the interface to user-level access permissions, click **File | Logoff**.

For more information about setting up logon accounts for NetCentral security, refer to [“Managing NetCentral security” on page 113](#).

Accessing NetCentral manager from a remote location

NetCentral clients can communicate with the NetCentral server via a Local Area Network, a Wide Area Network, or the Internet. If the client software is properly installed and configured as instructed in [Chapter 2, Installing the NetCentral system](#) and connecting systems are operational, you can operate NetCentral manager from a remote client PC just as you would from the NetCentral server PC.

You configure the NetCentral client interface to connect with a single NetCentral server PC when you install the client software. Only the NetCentral client component runs on a client PC. NetCentral services do not run on the client PC.

Stopping NetCentral

To stop the NetCentral interface, click **File** and choose **Exit**, or right-click the system tray icon and choose **Exit**.

When you stop NetCentral on a client PC, you are stopping only the client component. The server component on the server PC continues to run and the ongoing monitoring taking place on the server is not affected. Status change events from devices continue to be captured on the server and can be viewed from the client PC when the NetCentral client software is restarted.

When you stop NetCentral on the NetCentral server PC, you are likewise stopping only the NetCentral client component that runs on the server PC. The NetCentral server component continues to run and monitor your devices. Once NetCentral is started on the server, the server component does not stop unless you stop NetCentral services or shutdown the server. As long as the server component is running, if actions are configured, the actions are triggered and their notifications are executed. Of course, no messages can be displayed if the client component is not running, but messages received from devices are retained in the NetCentral database, so that when you again start the client component you can view the messages.

Also refer to [“Restarting NetCentral services” on page 128](#).

Adding NetCentral to startup

You can configure the Windows operating system to open the NetCentral interface automatically whenever the host PC starts.

The Windows 2000 procedure for adding NetCentral to startup is as follows. The procedure for your particular version of the Windows operating system might be different.

1. Right-click **Start** and select **Open All Users**. A window opens.
2. Double-click the **Programs** icon, then the **Startup** icon. A window opens for the Startup folder.
3. In the Startup folder window, right-click and select **New | Shortcut**. The Create Shortcut dialog box or wizard opens.
4. Browse to the NetCentral interface program file at the following location:

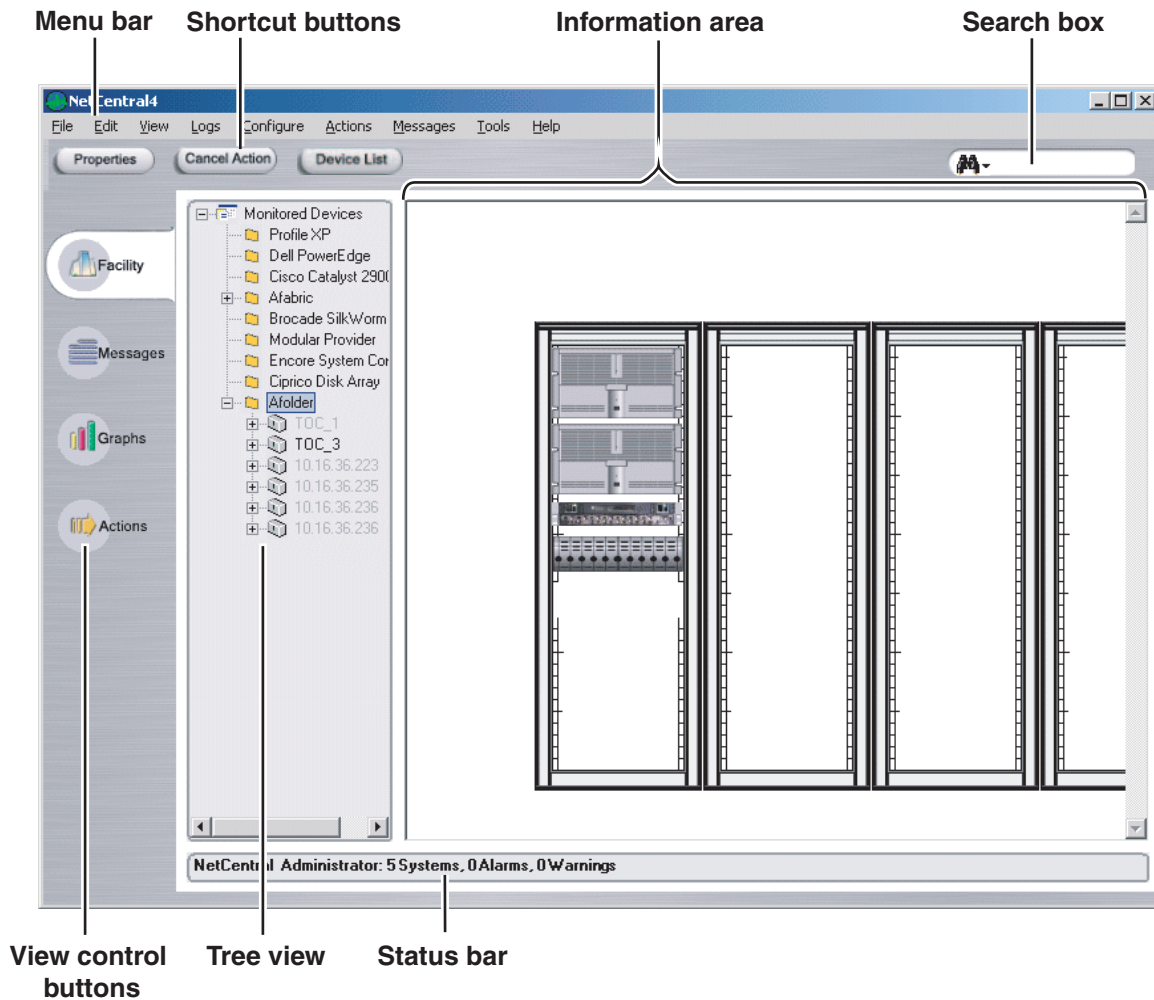
C:\Program Files\Thomson Grass Valley\NetCentral\bin\NetCentralIVFrontEnd.exe

Select the file and click **OK**.

5. Click the **Next** button, and then click the **Finish** button. The shortcut appears in the Startup folder window.
6. Close the Startup folder window. The next time you start the PC, the NetCentral interface opens automatically.

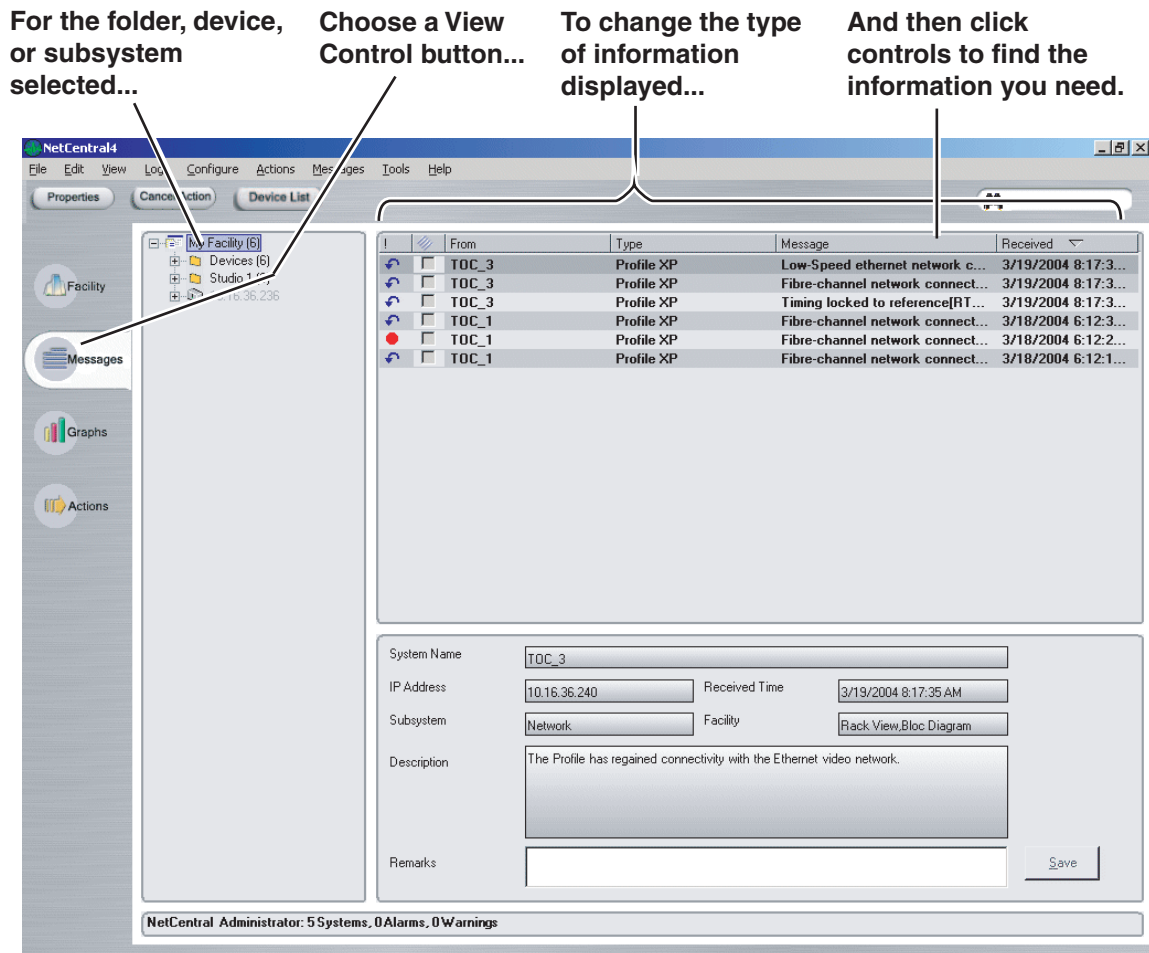
Overview of the NetCentral main window

The information in the NetCentral main window is arranged in different functional areas as follows:



Viewing information in the NetCentral main window

The NetCentral main window can be manipulated to display different views, as illustrated in the following screen shot:




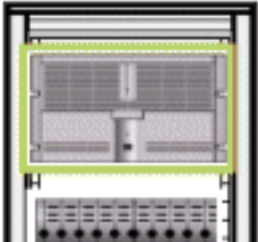


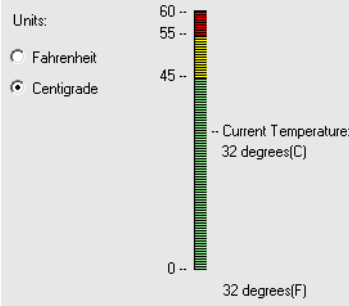
The views available in the NetCentral main window are described in the following topics.

- “Displaying the Facility view” on page 52
- “Displaying the Messages view” on page 53
- “Displaying the Graphs view” on page 53
- “Displaying the Actions view” on page 54
- “Displaying views in multiple windows” on page 54
- “Refreshing the information area” on page 54

Displaying the Facility view

With the Facility
view control
button selected...



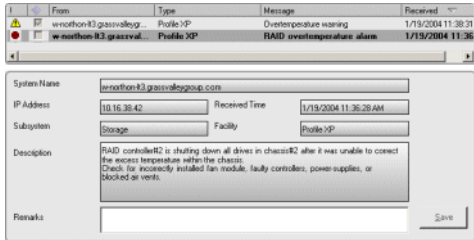
In the Tree view select this...	To display this view ...	Which provides this information.
 Folder		A HTML page with active graphics that display status indicators. You create this page to show your required logical or physical system view. Refer to “ Creating a Facility graphical view ” on page 57.
 Device	<div><div></div><div>10.16.36.223 IP Address: 10.16.36.223 Firmware Version: v2.2.1 Number of ports: 8</div></div> <div>Location: <input type="text"/></div>	General properties of the device.
..... Subsystem		Active graphics of the subsystem parameters.

To control the display of information in the Facility view, refer to “[Arranging the Tree
view](#)” on page 55 and “[Creating a Facility graphical view](#)” on page 57.

Displaying the Messages view

With the Messages
view control
button selected...



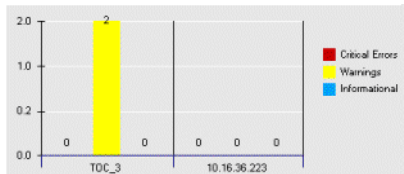
In the Tree view select this...	To display this view ...	Which provides this information.
Folder		Recent messages from devices and sub-folders contained in the selected folder. The lower pane displays the details for a selected message.
Device		Recent messages from the subsystems of the selected device. The lower pane displays the details for a selected message.
..... Subsystem		Recent messages from the selected subsystem. The lower pane displays the details for a selected message.

To control the display of information in the Messages view, refer to [“Defining messages displayed”](#) on page 70.

Displaying the Graphs view

With the Graphs
view control
button selected...




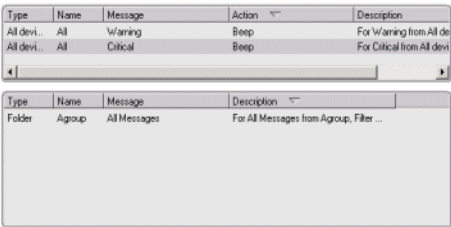

In the Tree view select this...	To display this view ...	Which provides this information.
Folder		Statistics in graphical form about the messages received from devices and sub-folders contained in the selected folder
Device		Statistics in graphical form about the messages received from the subsystems of the selected device.
..... Subsystem		Statistics in graphical form about the messages received from the selected subsystem.

To control the display of information in the Graphs view, refer to [“Defining information graphed”](#) on page 78.

Displaying the Actions view

With the Actions
view control
button selected...



In the Tree view select this...	To display this view ...	Which provides this information.
 Folder		Actions configured for the selected folder, its devices, and sub-folders. Filtered messages for the selected folder, its devices, and sub-folders are displayed in the lower pane.
 Device		Actions configured for the selected device and its subsystems. Filtered messages for the selected device and its subsystems are displayed in the lower pane.
..... Subsystem		Actions configured for the selected subsystem. Filtered messages for the selected subsystem are displayed in the lower pane.

Displaying views in multiple windows

You can extend the selection of different views beyond the main window and display more than one view at the same time. This is especially useful for computers with large screens or multiple screens.

To display multiple views do the following:

1. In the Tree view select a folder, device or subsystem.
2. Choose a View control button to display the view that you want.
3. Right-click the View control button or the selected folder, device, or subsystem and choose **Open In New Window**. The view opens in its own window.
4. Repeat this procedure to display different views. Arrange the windows as necessary.

Refreshing the information area

To refresh the information area for the currently displayed view, click **View** and select **Refresh**. You must refresh the view in this way when editing, saving, and viewing HTML pages.

Arranging the Tree view

By default, devices are grouped in the Tree view by type. If you require a different grouping of devices, use the procedures in this section.

The NetCentral interface allows you to group devices in the Tree view according to the following rules:

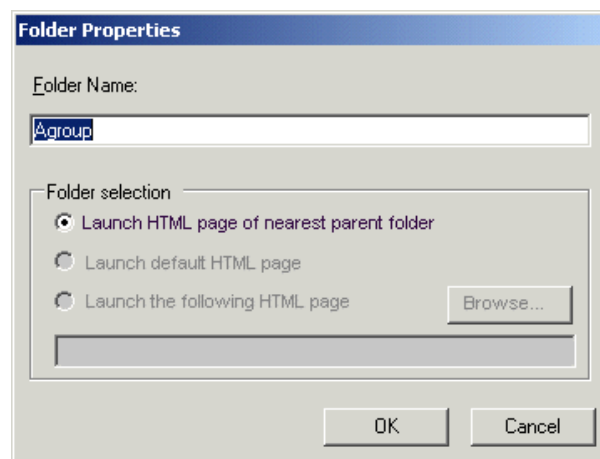
- Each group of devices must have a folder under which the group is defined.
- A device can be in multiple folders.
- You can nest folders under folders to create a hierarchical structure.
- You can not nest devices under devices.

Decide how you want to group your devices to more accurately represent your system environment, then proceed as follows:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Select the folder in the Tree View under which you want your new folder located.

To create a folder at the highest level possible, select the folder at the top of the tree. This folder is named *Monitored Devices* by default. You can rename this folder as required. You cannot create a folder above or at a peer level with this top-of-tree folder.

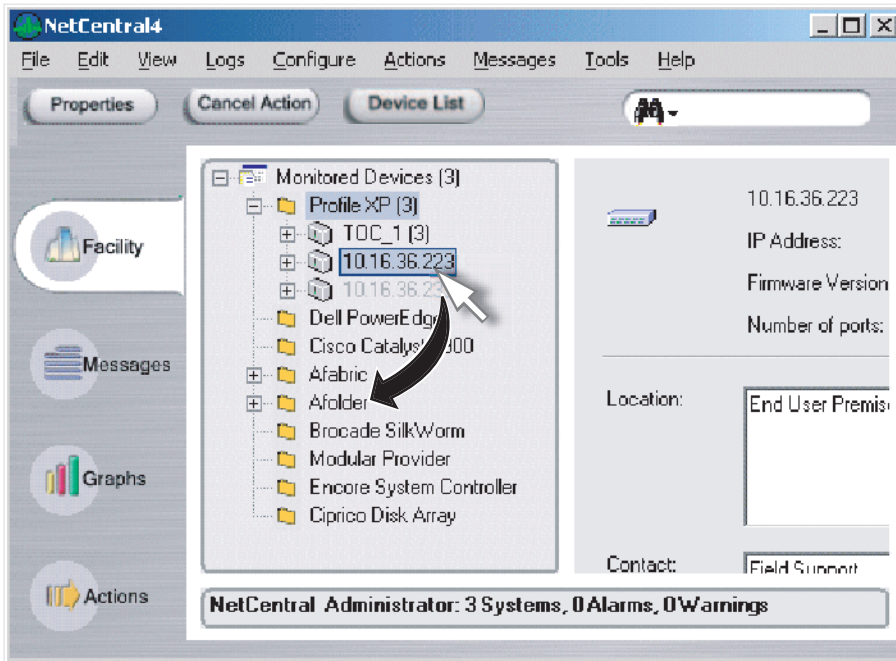
3. Click **File**, or right-click the folder, and select **Add | Folder**. The Folder Properties dialog box opens.



4. Enter a folder name that identifies the device group you are creating. Your new folder appears in the Tree view.

For now, leave other settings as default. Refer to [“Creating a Facility graphical view” on page 57](#) for instruction on associating the folder with a HTML page.

5. Within the Tree view, place devices into your new folder using one of the following methods:
 - Drag-and-drop to move a device into the folder
 - Select a device and click **Edit | Copy** or **Edit | Cut**, then select the folder and click **Edit | Paste**. You can right-click the device and folder and use the pop-up menu in the same way.



6. Repeat this procedure, creating a hierarchical structure of folders and devices as necessary to represent the systems and logical groupings in your facility.
7. Expand and collapse folders as necessary to view devices.
8. To remove a folder, move all devices out of the folder, right-click the folder and select **Delete**.

Searching for a folder in the Tree view

1. In the NetCentral Search box, click the binoculars icon and select **Folder**.



2. Enter text for the folder in the Search box and press **Enter**.

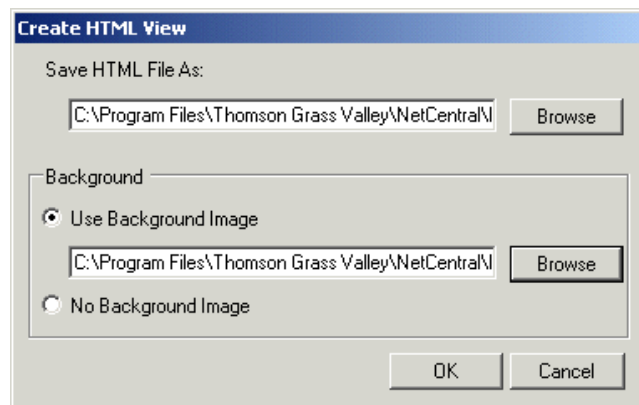
Creating a Facility graphical view

For any folder in the Tree view you can create a graphical view. The graphical view is displayed in the Facility view information area when the folder is selected. The graphical view is actually a HTML page upon which active drawings are arranged, typically to represent the devices in the folder.

Use the following procedure to create a basic HTML page with a representation of your monitored devices in racks. If you are knowledgeable about HTML and images, you can create other customized background pages to represent networks, functional groups, or other views of your monitored devices. To understand how to integrate these advanced HTML techniques with NetCentral, refer to [Appendix A, Graphical view tutorial on page 133](#).

To create a HTML graphical view of a folder, do the following:

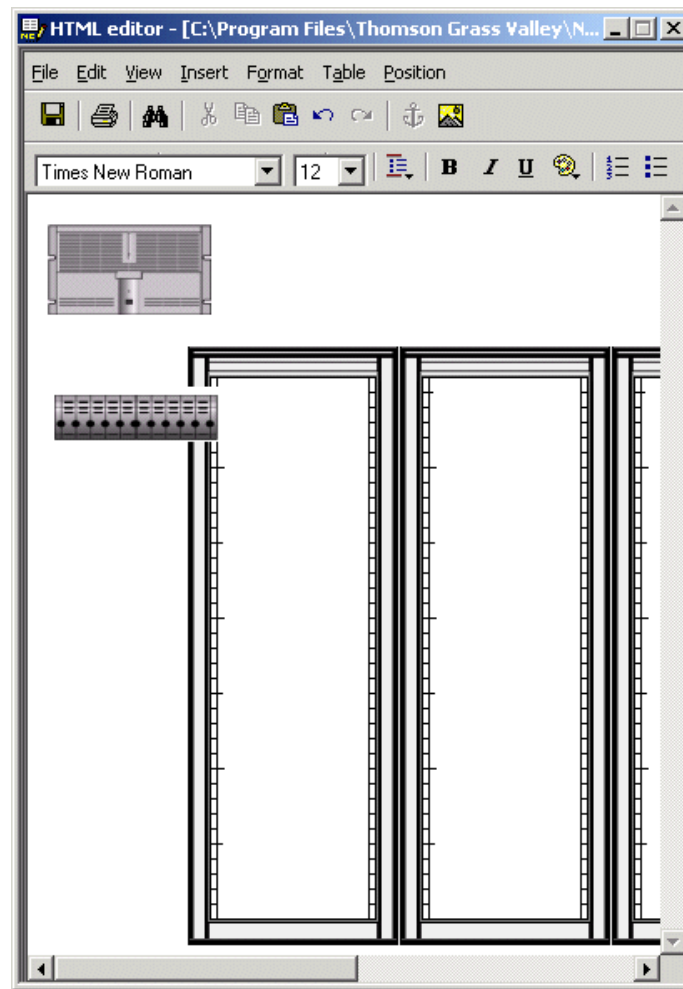
1. On the NetCentral server PC, open the NetCentral interface and log on to NetCentral with administrator-level privileges.
2. Select the folder for which you are making the graphical view. In this procedure, the folder is named *MyFolder*. Right-click and select **Create HTML View**. The Create HTML View dialog box opens.



3. Select **Use Background Image**, then click **Browse** and select the following file:
C:\Program Files\Thomson Grass Valley\NetCentral\HTML\4Racks_36RU_Small.gif

This creates a HTML file named *MyFolder.html* that displays *4Racks_36RU_Small.gif* as a background image.

4. Click **OK**. The NetCentral HTML editor opens.



The HTML page is automatically loaded into the HTML editor. The rack drawings are the background image. On top of the background image are the active drawings of the devices and/or sub-folders in the folder.

5. Select the active drawings and position them on the background image, so they appear as devices in racks.
6. You can also enter text to identify the HTML page.
7. In the HTML editor, save the page, then close the HTML editor.
8. In the NetCentral main window, the HTML page is displayed in the information area when the folder is selected. Hover your cursor over an active drawing to display the name of the active drawing as a tooltip.
9. If you have NetCentral client PCs, copy *MyFolder.html* and *4Racks_36RU_Small.gif* to each of your NetCentral client PCs so that the files are in the same location on each NetCentral client PC as they are on the NetCentral server PC.

If you remove a device from a Tree view folder, and that device is represented as an active drawing on the folder's HTML page, you must manually edit the HTML page to remove the active drawing. To do this right-click the folder in the Tree view and select **HTML Page**. This opens the page in the NetCentral HTML editor. After editing the HTML page, right-click in the information area or click **View** and select **Refresh**.

For advanced graphical view features, refer to [Appendix A, Graphical view tutorial on page 133](#).

As you navigate your HTML pages, you can move forward and backward along the sequence of HTML pages that you have viewed. To do this, right-click on a HTML page background (not on an active drawing) and select **Forward** or **Back**.

Interpreting status indicators

The following topics explain the primary graphical conventions that NetCentral manager software uses to inform you of device status:

- [“About status indicators” on page 60](#)
- [“Locating status indicators in the NetCentral main window” on page 61](#)
- [“Interpreting grayed-out devices” on page 61](#)
- [“Viewing status in the system tray icon” on page 62](#)

About status indicators




The NetCentral system categorizes any information it receives from devices as one of the following status levels. The status levels and the default icons that represent them are as follows:

Informational		A device has experienced a change in status within normal operating parameters. The device is operating as designed.
Warning		A device has a reduced ability to function and may fail soon, but at the current moment it is still operating within specifications as designed.
Critical		A device has ceased to operate or is currently operating with severely hampered functionality. The device is not operating within specifications as designed.
Reset		A device has returned to normal operating status. A previous warning or critical status condition has been resolved.
Dead or off-line		A device is not operating at all or has lost contact with the NetCentral system.

The NetCentral system indicates these status levels throughout the interface, using the following default icons, colors, animations, and actions:

	Informational	Warning	Critical	Reset	Dead or Off-line
System tray icon	Green heartbeat	Red heartbeat	Red heartbeat	Green heartbeat	Red heartbeat
Main window Tree view					
Main window Messages view					
Default action	None	NetCentral window maximizes, Beep sounds	NetCentral window maximizes, Beep sounds	None	NetCentral window maximizes, Beep sounds

Also, for subsystem properties in the Facility view, some devices use a “colored light” graphic to indicate status. The meaning of the light is as follows:

- Green light  — Normal
- Red light  — Fault
- Black  — Information not available, no communication, or no signal detected

The following sections contain more detailed information about status indicators.

For Syslog monitoring, refer to [“Setting up and using Syslog in NetCentral” on page 43](#).

Locating status indicators in the NetCentral main window

Device status is indicated within the different areas and views as follows:

Tree view — This hierarchical list groups devices and their subsystems under nested folders. Status indicators replace the icon for a folder, device, or subsystem if status is not normal. Status indicators “ripple up” through the hierarchy, so that even if you have a folder closed in which multiple devices or folders reside, a status indicator on the top folder indicates the status of highest severity amongst all the folder’s contents. Read [“Arranging the Tree view” on page 55](#) for more information.

Information area: Facility view — This view displays folders, devices, or subsystems as graphics. Status indicators in the Facility view can take various forms. By default, active drawings change color to indicate status.

Information area: Messages view — This view displays messages received. The messages explain status changes and, if necessary, give suggestions for corrective action. Status indicator icons appear in the “!” column, which by default is in the left-most position.


Information area: Actions view — This view displays actions configured. It identifies the status change that triggers each action. Actions are highlighted if they are currently being triggered, such when a beep tone or audio file sounds. You can use this as a status indicator by tracing the action to the status change that triggered it.

Interpreting grayed-out devices

NetCentral displays a device in a grayed-out state to communicate information about the device as follows:

- In the Tree view, if a device name or IP address appears in a grayed-out state, it means that the device is not currently sending its SNMP trap messages to the NetCentral server. A tool tip displays this information when you hover your cursor over the device icon. Refer to [“Verify SNMP trap messages from monitored devices” on page 38](#).

Viewing status in the system tray icon

As long as the NetCentral interface is open, you will see the NetCentral icon  in the system tray of the NetCentral server PC's Windows taskbar. The moving heartbeat in the icon provides visual confirmation that the NetCentral system is operational, using the following colors to indicate device status level:

Green = All devices are at a Normal, Informational, or Reset status level

Red = One or more devices are at a Warning, Critical/Dead, or Off-line status level

If more than one device is being monitored, the color indicates the status level of highest severity. For example, if a Profile XP Media Platform has a informational status and a QLogic Fibre Channel switch simultaneously has a warning status, the NetCentral system displays a red color heartbeat to indicate the warning status of the QLogic Fibre Channel switch, since it is of higher severity.

Responding to messages and actions

The following topics explain how the NetCentral manager interface behaves and how you can respond when messages are received from monitored devices:

- [“Interpreting NetCentral messages” on page 63](#)
- [“Acknowledging messages” on page 64](#)
- [“Clearing acknowledged messages” on page 64](#)
- [“Clearing alarms” on page 64](#)
- [“Clearing warning and critical icons” on page 65](#)

Interpreting NetCentral messages

The NetCentral system notifies you immediately if any of your devices reach a status-level of critical or warning by sounding an audible beep. Other actions can be triggered as well, such as playing a sound file or sending an e-mail message. For information on triggering other actions, see [“Configuring actions and notifications” on page 87](#).

The message details, as displayed in the Messages view, offer suggestions as to what you might do to resolve the condition that triggered the alarm, as in the following example:

Description	One or more system cooling-fans have failed or the fan assembly has been removed. Replace the fan assembly.
-------------	---

To quickly see a device’s messages from a Facility view HTML page, right-click the device’s active drawing and select **Messages**. The device’s messages open in a new window.

In most cases you should act immediately to resolve warning or critical conditions. For more information about troubleshooting a particular device, refer to the manual for that device.

Once the condition is resolved, the NetCentral system sends a reset message to notify you that the device has returned to normal status, as in the following example:

Description	The system cooling-fans resumed normal operation.
-------------	---

The reset message removes the related alarm or critical icon, so the device appears again as normal.

Acknowledging messages

When a message is first received from a device it is considered an unacknowledged message and as such it is displayed in the Messages view as bold text. In the Tree view, the associated subsystem, device, and folders display a number in parentheses that indicates the current number of unacknowledged messages. These are your indicators that the one or more messages are recent and possibly un-read. To acknowledge that a message has been read, in the Messages view double-click the message row. This puts a checkmark in the checkbox and changes the text to a normal font appearance.

Clearing acknowledged messages

If you find your acknowledged messages cluttering the Messages view, you can clear them from the viewing area as follows:

- Click the acknowledged message checkbox column head one or more times until acknowledged messages are sorted to the bottom of the list and outside of the primary viewing area.
- Click **Configure | View Settings** and de-select **Show Acknowledged Messages**. The acknowledged messages disappear from the Messages view. If you have a large number of messages and you find performance is affected as they fill the list, setting this option and acknowledging past messages can boost performance. The acknowledged messages are retained in the NetCentral database, so you can always view them again by resetting the option to show acknowledged messages in the Messages view.

Clearing alarms

The Cancel Actions shortcut button flashes when a cancellable alarm is present. To turn off most types of alarms, click the **Cancel Actions** button or choose **Actions | Cancel Actions**.

You can also turn off individual Actions as follows:

1. Display the Actions view.
2. Select the folder, device, or subsystem from which the action is currently executing. If you are not sure, click the topmost folder. Actions are displayed in the information area. Currently executing actions are displayed in bold text.
3. In the Information area, identify and select the action or actions currently executing.
4. Click **Actions | Cancel Actions | Selected**, or right-click the action row and select **Cancel Action**.

This turns off the alarm while you take steps to correct the problem.

Once the action is cancelled or is finished, the only indication that the warning or critical condition still exists is the color of the system tray icon and the message and status icons in the NetCentral window. The NetCentral system itself does not send messages or trigger actions again to remind you of a current warning or critical condition. However, some devices have a feature, such as the “Resend Messages”

feature on a Profile XP Media Platform, that you can configure to have the device send a message again for an unresolved condition. Check the manual for your device for more information about this type of feature.

If some messages become troublesome because they are too frequent or unimportant, you can set the NetCentral system to filter certain messages. For more information, see [“Filtering messages to disable actions” on page 100](#).

Clearing warning and critical icons

It is possible that a currently irrelevant message can cause a device to continue to display a warning or critical icon. You can remove the warning or critical icon from the device in the Tree view by right-clicking the device and selecting **Reset State**. You must be logged on to NetCentral with technician-level or administrator-level privileges to reset the state of a device in this way.

Finding monitored devices

Use the following procedures to locate SNMP-monitored devices that might be otherwise difficult to find.

- “Searching for a device” on page 66
- “Viewing a simple list of devices” on page 66

Searching for a device

1. In the NetCentral Search box, click the binoculars icon and select **Device**.

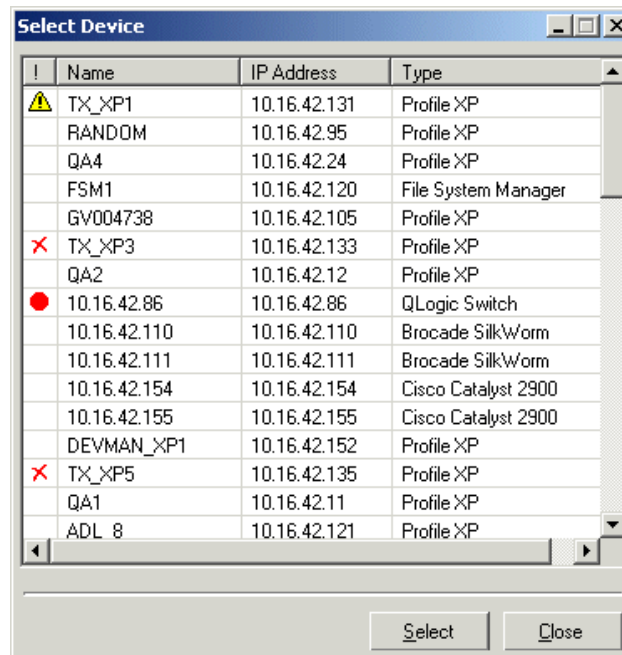


2. Enter text for the device name in the Search box and press **Enter**.

Viewing a simple list of devices

If you are not sure of the location of your devices in the Tree view, you can view a non-hierarchical list of all currently monitored devices, in which each device is listed just once.

1. Click the **Device List** button or click **Tools | Device View**. The Select Device dialog box appears.



2. Click column heads to sort and drag column heads to rearrange.
3. Double-click a device row, or select a device row and click **Select**. The Select Device dialog box closes and the device is selected in the Tree view.

Browsing device status

At any time you can view status information for a SNMP-monitored device as explained in the following topics:

- [“Viewing subsystem properties” on page 67](#)
- [“Viewing general information for a device” on page 67](#)

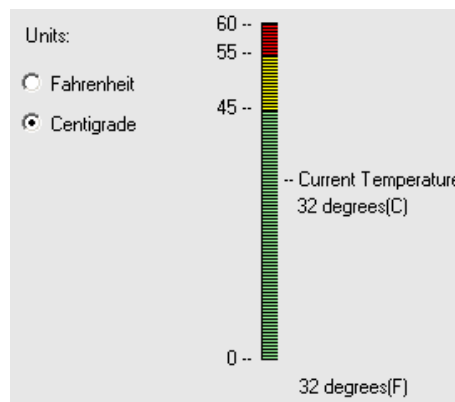
For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 42](#)

Viewing subsystem properties

The Information area can display a detailed view of the properties for a subsystem and its status. To display this information do the following:

1. In the Tree view, select a subsystem under a device.
2. Select the **Facility** View control button. The Information area displays icons and graphics that provide indicators of subsystem status.

For example, the properties for a thermal subsystem are illustrated as a thermometer image.



3. Click controls to sort, filter, or arrange information. For example, for the thermal subsystem you can select the units in which you want the temperature displayed.

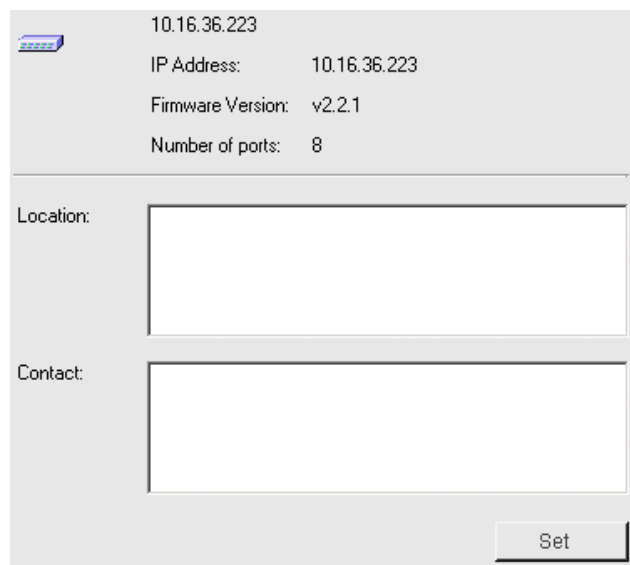
If a status parameter changes on a monitored device while the related subsystem properties remain displayed, the change might not be propagated to the displayed properties for up to thirty seconds or until the properties are re-displayed.

Read the device’s manual for documentation on its NetCentral sub-system pages.

Viewing general information for a device

To view general information, do the following:

1. In the Tree view, open a device and select the **System** sub-system.
2. Select the **Facility** View control button. The Information area displays IP address, location, and other general information.



A screenshot of a NetCentral configuration window for a device. The window has a light gray background. At the top left is a small icon of a network device. To its right, the IP address '10.16.36.223' is displayed. Below this, the following information is listed: 'IP Address: 10.16.36.223', 'Firmware Version: v2.2.1', and 'Number of ports: 8'. A horizontal line separates this information from the configuration fields below. There are two large, empty text input boxes. The first is labeled 'Location:' and the second is labeled 'Contact:'. At the bottom right of the window is a button labeled 'Set'.

10.16.36.223
IP Address: 10.16.36.223
Firmware Version: v2.2.1
Number of ports: 8

Location:	
Contact:	

Set

3. In the Location and Contact boxes, if you are logged in with appropriate permissions, you can fill in the information appropriate for that particular device. Click **Set** to put changes into effect.

Researching device status in NetCentral messages

The NetCentral messages that appear in the Messages view are SNMP trap messages and messages from other protocols that monitored devices send when they experience a status change. The messages are stored in the NetCentral database on the NetCentral server PC. As long as NetCentral is running on the server PC all messages from devices are captured and stored. As the NetCentral system monitors your devices over time these messages form a pool of data that you can research.

When the NetCentral database approaches its maximum size limit, the oldest messages are purged. Refer to [“Accommodating NetCentral database growth” on page 118](#).

The primary tool to access the NetCentral message database is the Messages view. By using Messages view features as explained in the following sections you can manipulate the display of messages to conduct your research, as explained by the following topics:

- [“Researching messages” on page 69](#)
- [“Defining messages displayed” on page 70](#)
- [“Rearranging message information” on page 71](#)
- [“Grouping messages” on page 71](#)
- [“Searching messages” on page 72](#)

Refer to [“About logs that contain NetCentral system information” on page 128](#) to research messages about the NetCentral system itself.

Researching messages

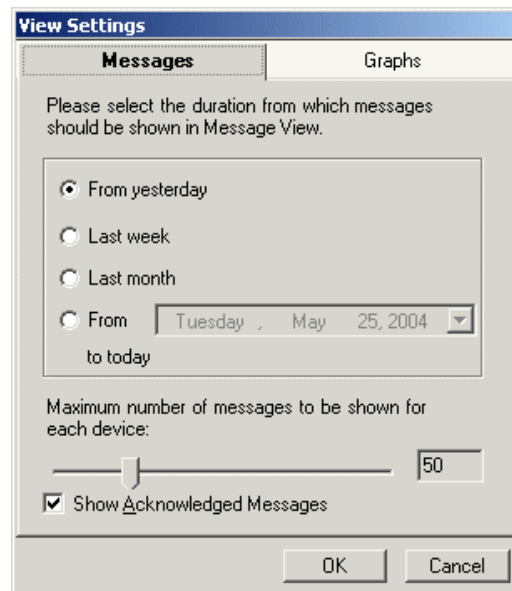
NetCentral offers several mechanisms for researching messages, depending on the range of information you need, as follows:

- **Recent messages** — By default, the Messages view displays the most recent messages only. You can rearrange the display of this message information within the main Messages view by simply clicking on column heads and dragging columns. You can also set a shorter or longer past time period to display more or less messages. Refer to [“Defining messages displayed” on page 70](#).
- **Past messages** — These are messages that are no longer displayed in the main Messages view but that have not yet been compressed. These messages are retained in the NetCentral database with all their text and associated remarks for full research.
- **Message statistics** — This is statistical information about all the messages NetCentral has received since it was first installed. This includes the past and recent messages that are currently in the NetCentral database, as well as the compressed messages that have been purged from the database. The statistical information is displayed as graphs. Refer to [“Researching device status with graphs” on page 77](#).

- Compressed messages — These are your oldest messages. NetCentral automatically purges these messages when the NetCentral database gets too full of messages. The information for research from these messages is available only in its compressed form, as displayed in the message statistic graphs. Refer to [“Accommodating NetCentral database growth” on page 118](#).

Defining messages displayed

1. Select a folder, device, or subsystem to display the group of messages in the Messages view in which you are interested. By default only recent messages are displayed.
 - If the time period and number of the recent messages currently displayed is sufficient for your research, you can click column heads and rearrange columns to find the information you need.
 - If the time period and number of the recent messages currently displayed is not sufficient for your research, continue with this procedure.
2. Click **Configure | View Settings**. The View Settings dialog box opens.



3. Click the **Messages** tab.
4. Configure the past time period for which you want messages displayed.
5. Adjust the slider bar to specify the number of messages displayed per device. This takes effect when a folder that contains multiple devices is selected, so that you are sure to see the most recent messages from each device in the folder.
6. Specify if acknowledged messages are displayed.
7. Click **OK** to save settings and close.

Rearranging message information

You can rearrange the message information in the Messages view by manipulating columns, which are as follows:

- Severity
- Acknowledged
- Device Name
- Device Type
- Message name
- Date and time received

To rearrange message information, do the following:

1. Select a folder, device, or subsystem to display the group of messages in the Messages view in which you are interested.
2. Click a column head to sort messages by the contents of that column. Click again to sort in reverse order.
3. Click and drag column side borders to re-size columns.
4. Click and drag column heads to re-arrange columns.

Grouping messages

As you arrange folders and devices in the Tree view you are also grouping how messages are displayed in the Messages view. For example, when you select a folder and display its Messages view, only the messages from the devices in that folder are displayed. This effectively filters out messages from other devices. You similarly group messages by device or by subsystem when you select a device or a subsystem in the Tree view.

If your current arrangement of folders and devices does not group device messages as necessary for your research needs, you can set up some special folders just for the purpose of grouping device messages. Since multiple instances of a single device can reside in multiple folder, setting up special folders like this does not interfere with other monitoring requirements.

To set up a folder for grouping device messages, do the following:

1. In the Tree view, create a folder and name it for the group of device messages you need. For example, if you want to group messages from all devices that supply media for a particular function, you could name the folder with the function's name.
2. Copy into the folder all the devices whose messages you want to group. You can also copy in other folders, which adds the messages from those folder's devices to your group.
3. Select your folder and click the **Messages** view control button. The messages from all your grouped devices appear. You can now continue your research by sorting and arranging the messages in the group.

Searching messages

Use the following procedure to locate text in a message that might be otherwise difficult to find.

1. Make sure the Messages view is currently displayed.
2. In the NetCentral Search box, click the binoculars icon and select **Message**.



3. Enter text for the message in the Search box and press **Enter**. This searches in each message the text that appears in the “Message” column in the Messages view.

Exporting NetCentral messages

You can export message information from the NetCentral database and write it to a file. This is useful for printing messages or for using the exported message information in other applications for further manipulation and research.

You must be logged on to NetCentral with technician-level or administrator-level privileges to export messages.

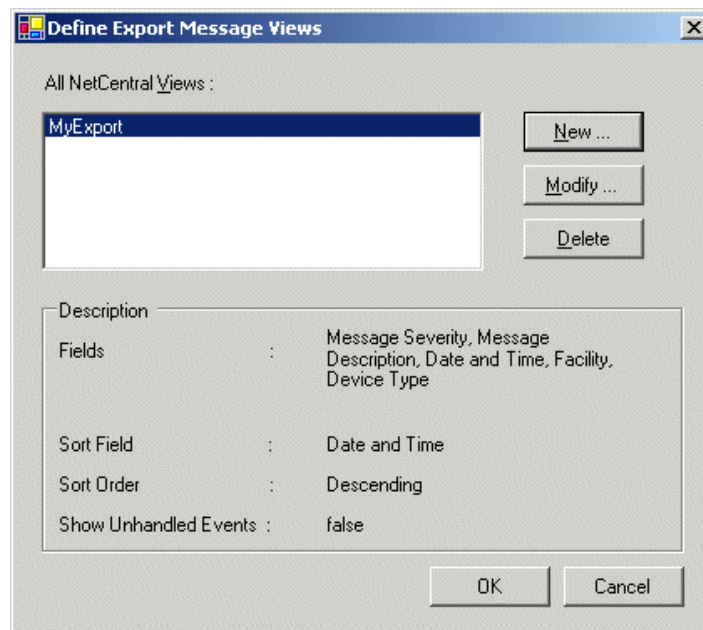
The following topics explain how to export NetCentral messages:

- [“Setting the export view” on page 73](#)
- [“Exporting messages” on page 74](#)
- [“Defining an export query” on page 75](#)
- [“Printing messages” on page 76](#)

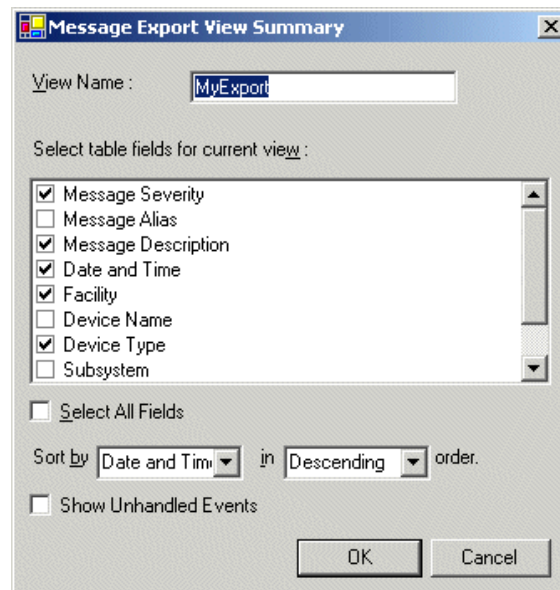
Setting the export view

Before you export message information, you must define the view in which it is exported, as explained in the following procedure.

1. Make sure you are logged on to NetCentral with technician-level or administrator-level privileges.
2. Click **Messages | NetCentral Messages | Define Export Views**. The Define Export Message Views dialog box opens.



3. Click **New**. The Message Export View Summary dialog box opens.



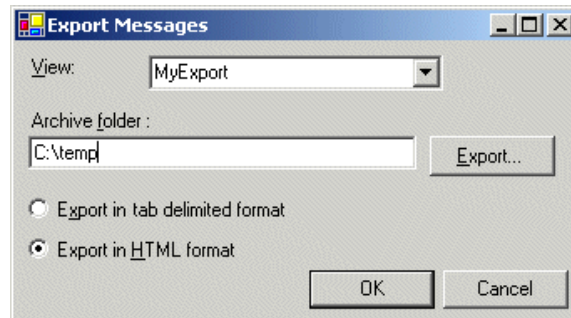
4. Enter a name for the view you are defining.
5. Define the view as follows:
 - Select the columns of information to include in your exported messages.
 - Specify the sort order of the messages
 - Select Show Unhandled Events to include SNMP trap messages received from devices for which there is not a corresponding NetCentral message.
6. Click **OK** to save settings and close.
7. Your view is listed in the Define Export Message Views dialog box. Use the New, Modify, and Delete buttons to create a list of views for exporting messages as you require.
8. On the Define Export Message Views dialog box, click **OK** to save settings and close.

Exporting messages

You can export messages to a file as follows:

1. Make sure you are logged on to NetCentral with technician-level or administrator-level privileges.

2. Click **Messages | NetCentral Messages | Export**. The Export Messages dialog box opens.

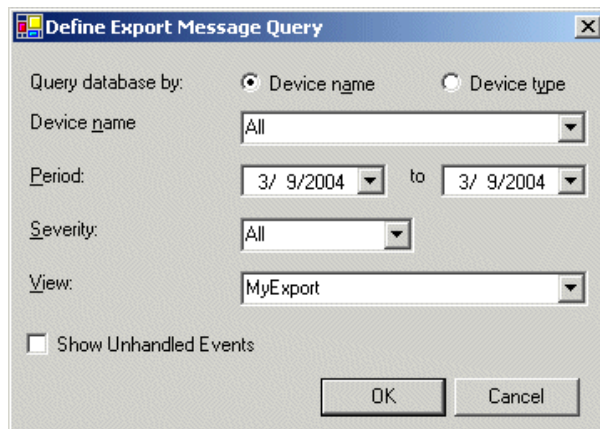


3. Select the view in which to export the messages.
4. Specify the location to which the exported file is saved.
5. Select the format for the exported file.
6. Click **OK** to save settings and close. The export file is generated, named according to the time and view name, saved to your specified location, and displayed as defined for export format.

Defining an export query

You can export a sub-set of messages by defining a query, as follows:

1. Make sure you are logged on to NetCentral with technician-level or administrator-level privileges.
2. Click **Messages | NetCentral Messages | Define Export Query**. The Define Export Message Query dialog box opens.



3. Build your query to define the set of messages you want included in your export.
4. Select the view in which you want the exported messaged information arranged.
5. Click the **OK** button. Messages are displayed as a HTML page, as defined by the query.

Printing messages

To create a report of messages that can be printed, first define message export views or queries, as explained in procedures earlier in this section. Then export the file, which makes the message information available for printing.

If you export in HTML format, you can print directly from your Web browser. Alternatively, you can open an exported file using an application from which you can format the information. For example, if you exported in tab delimited format, you can import into a spreadsheet application and modify the spacing and arrangement of the message information so as to make it suitable for printing.

Researching device status with graphs

The Graphs view compiles statistics about all the messages NetCentral has received since it was first installed and presents the results as charts and graphs. These charts and graphs show a summary of the recent, past, and compressed message information in the NetCentral database. Refer to [“Accommodating NetCentral database growth” on page 118](#). With this type of presentation, long-range trends can be identified that would otherwise be difficult to research.

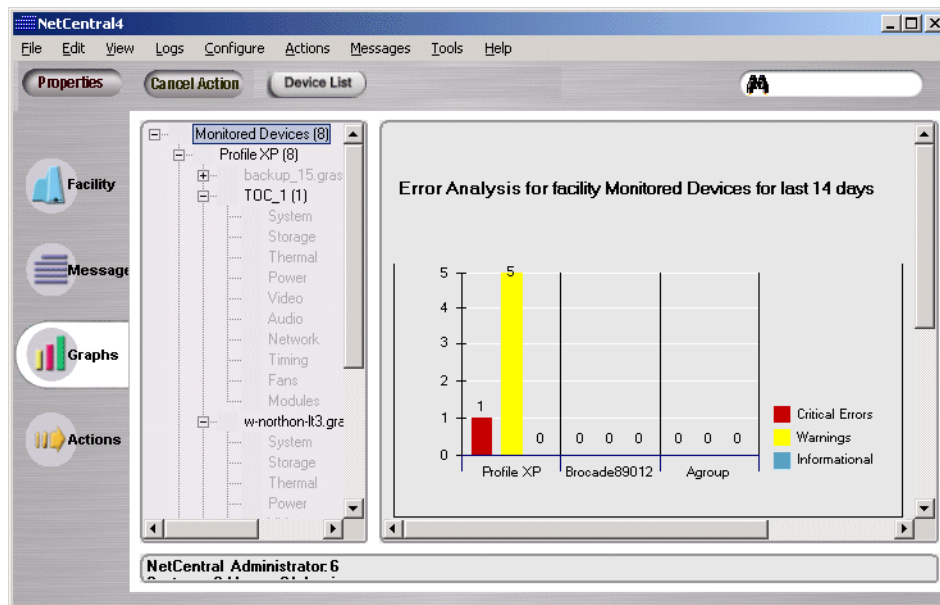
The following topics explain how to use NetCentral graphs:

- [“Viewing statistical graphs” on page 77](#)
- [“Defining information graphed” on page 78](#)

Refer to [“About logs that contain NetCentral system information” on page 128](#) to research information about the NetCentral system itself.

Viewing statistical graphs

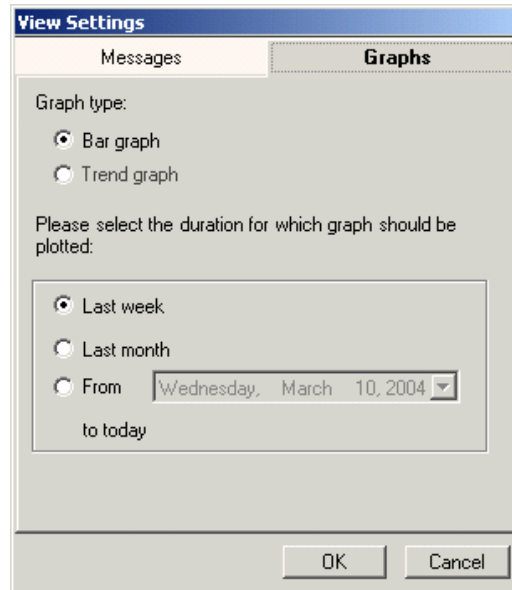
1. Select the **Graphs** view control button.
2. In the Tree view, select a folder, device, or subsystem for which you want to view the statistical graph. The graph appears in the information area.



Defining information graphed

You can change the setting for the time period of messages information graphed, as follows:

1. Click **Configure | View Settings**. The View Settings dialog box appears.



2. Click the **Graphs** tab.
3. Select the graph type.
4. Select the time period for which you want messages graphed.
5. Click **OK** to save settings and close.

Researching device-specific logs

Device-specific logs reside on the monitored device. Some device-types have these logs and make them available to the NetCentral system, while others do not. The number and nature of these logs varies from device to device.

If a device-type supports NetCentral's device-specific log feature, each device of that type must be set up with a mechanism for making its logs available to the NetCentral server. For example, on a Profile XP Media Platform a File Transfer Protocol (FTP) server makes the logs available for FTP download to the PC running NetCentral. Refer to the documentation for the device for instructions on setting up the required log mechanism on the device.

Since device-specific logs are downloaded to the PC running NetCentral, they do not automatically refresh to show new entries. You must download a new copy of the log to see new entries.

The following topics explain how to use the NetCentral system to download and view logs.

- [“Viewing a single device-specific log” on page 79](#)
- [“Downloading multiple device-specific logs” on page 80](#)

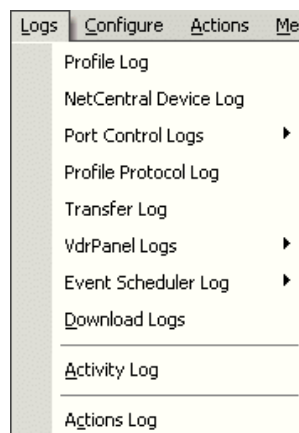
Refer to [“About logs that contain NetCentral system information” on page 128](#) to research information about the NetCentral system itself.

Viewing a single device-specific log

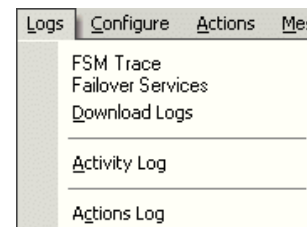
You can view a device-specific log using the NetCentral interface. The NetCentral system automatically downloads only the log you selected and then opens the log automatically, as explained in the following procedure.

1. In the Tree View, highlight the device for which you want to view log information.
2. Click **Logs** and select the log you want. Device-specific logs are listed at the top of the menu. Each type of device has their own list of logs, as illustrated by the following menus:

Profile XP Media Platform



Open SAN FSM



The NetCentral system downloads the log you select to the PC running NetCentral and opens it automatically.

While the log remains open it does not refresh to show new entries.

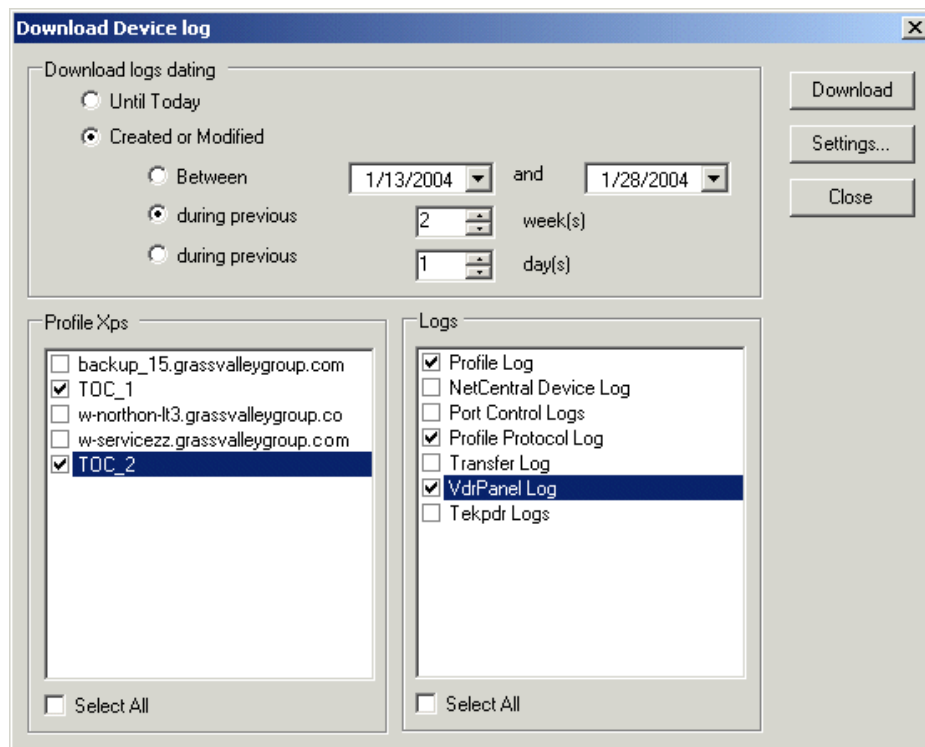
3. To view new entries in the log, close the log and repeat this procedure.

NOTE: The settings available from the Download Device log dialog box, as explained in the next procedure, apply to the download of single device-specific logs. If there is a problem downloading a single device-specific log, check these settings as well as the download mechanism (such as FTP) on the device.

Downloading multiple device-specific logs

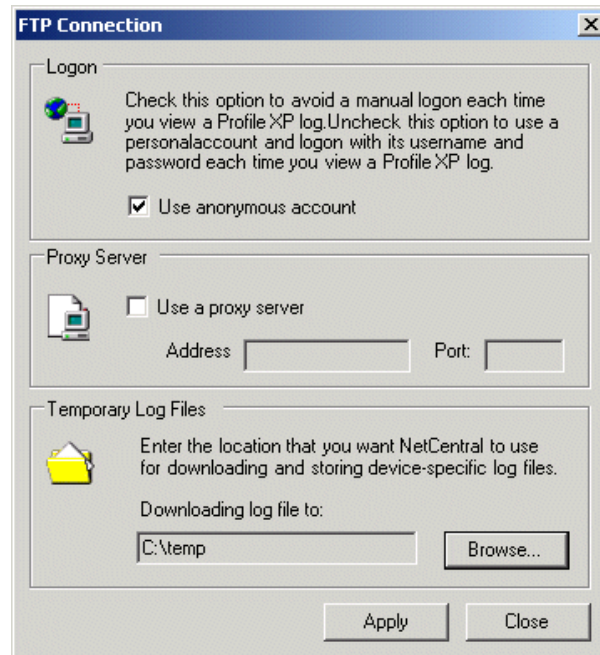
You can download logs in a batch and save them to a directory on the PC running NetCentral. From this directory you can then open and view the logs using applications such as Notepad, as explained in the following procedure.

1. In the Tree view, select a device of the device-type from which you want to download logs.
2. Click **Logs | Download Logs**. The Download Device log dialog box opens.



3. Configure the date settings to target the information in which you are interested.
4. Select the devices from which you want to download logs.
5. Select the logs that you want to download from the devices you have selected.
6. Click **Settings**. A dialog box appears that allows you to configure the settings for

the log download mechanism (for both for single log download and batch log download) used by the particular device. For example, FTP is used by many devices for log downloads, so the FTP Connection dialog box allows you to configure settings.



7. Verify that settings are configured as necessary for downloads. In most cases the default settings are sufficient.
8. Click **Apply** and **Close** to save settings and close.
9. On the Download Device log dialog box click **Download**. A Device Log Transfer dialog box appears that indicates progress.
10. When the download process is complete, NetCentral displays a report of the logs downloaded. You can identify devices that are not properly configured for log downloads by the results in this report.
11. Navigate to the log download directory and open logs as desired using Notepad or another text editor.

The copies of logs on the PC running NetCentral that are downloaded and viewed in this way do not refresh to show new entries, even if you close and re-open the logs.

12. To view new information, close the logs and repeat this procedure.

Using device-specific features

With the NetCentral system you can access features and applications that are specific to a particular type of device. When a device is selected in the Tree view, that device exposes its features through the NetCentral interface menus. In this way different types of devices fill in the menus differently. To see a menu that exposes any special features a device-type might have, right-click the device in the Tree view.

For information about using a device-specific feature or application, read the manual for that particular device.

Viewing version information

You can generate a report of version information for the device currently selected or for all the devices in the folder currently selected, as follows:

1. Select the device or folder for which you want version information.
2. Click **View | Versions**. The Export Versions dialog box opens.
3. Specify the location of the exported file, select the format for the report, and click **OK**. A message box shows progress as the report is generated. If the format is HTML, the report opens as a HTML page in your browser window.

VERSION INFORMATION

DeviceName	IPAddress	Device Model	Operating System	Profile System Software	Drive Micro Code	Control Video Flare	Chassis Model
TOC_1	10.16.36.230	PVS1024	Hardware: x86 Family 6 Model 5 Stepping 2 AT/AT COMPATIBLE - Software: Windows NT Version 4.0 (Build Number: 1381 Uniprocessor Free)	5.4.1.71.	ClickHere	ClickHere	ClickHere

TOC_1- Drive Micro Code Values

Chassis Id	Controller ID	Drive ID	Drive Micro Code
0	1	0	3528

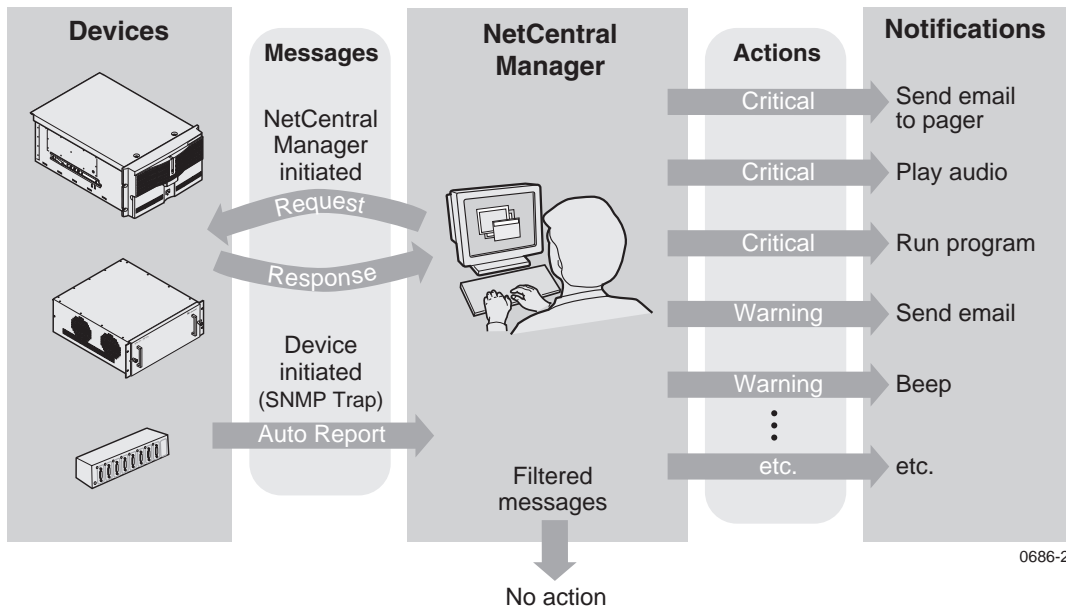
Managing messages and actions

Upon installation, the NetCentral manager interface uses default settings to manage the receipt, distribution, and notification of the status information it receives from monitored devices. This section explains how you can change these settings to better suit the systems and policies in your particular environment. Topics are as follows:

- [“About messages and actions” on page 84](#)
- [“Configuring messages” on page 85](#)
- [“Configuring actions and notifications” on page 87](#)
- [“Filtering messages to disable actions” on page 100](#)

About messages and actions

The following diagram illustrates how messages and actions interact in the NetCentral system.



Messages — Devices communicate to NetCentral manager about their status using messages. Some messages are initiated by the manager software, in that the device sends the message only when the manager software requests. Other messages, such as SNMP traps, are initiated by the device, in that the message is sent whenever a change in status occurs on the device.

Actions — The NetCentral system notifies to you about the status of devices using actions. By configuring actions you can create a customized set of notifications.

For Syslog monitoring, refer to [“Monitoring with multiple protocols”](#) on page 42.

Configuring messages

There are two types of messages that appear in the NetCentral interface. The different types of messages use different mechanisms for configuring when and how the message is sent. The type of messages are as follows:

- **NetCentral manager initiated messages** — These messages carry information about a particular monitored device, yet they only occur when they are triggered by the NetCentral manager software. As such, these messages can be controlled by the manager software. NetCentral manager initiated messages are as follows:
 - **Heartbeat polling** — This is when a device does not respond to the manager software's heartbeat polling and a "Dead or off-line" message appears in the Messages view. Refer to ["Setting heartbeat polling" on page 111](#).
- **Device initiated messages** — These are the SNMP trap messages or other monitoring protocol messages that are triggered by each device. This type of message is sent when a threshold condition occurs on a device and the status of the device changes. As such, the mechanisms for the control of these messages varies from device to device. Read the manual for the particular device-type for more information. Some examples are as follows:
 - Some types of devices have features within the device interface that allow you to set the parameters for threshold conditions.
 - Some types of devices expose settings of this type through the NetCentral manager Device menu, such as the Device Options dialog box for a Profile XP Media Platform.

The following topics describe how to configure messages:

- ["Adding remarks to messages" on page 85](#)
- ["Copying messages" on page 86](#)

Adding remarks to messages

Once a message is received from a monitored device, you can add, edit, or remove remarks associated with the message. The remarks are retained with the message in the NetCentral database and are available for research.

Adding or editing a remark

To add or edit a remark, do the following:

1. In the Messages view, display the message to which you want to add or edit a remark.
2. Enter or edit text in the **Remarks** field at the bottom of the message details pane.

From	Type	Message	Received
w-northon-lt3.grassval...	Profile XP	Fan Fault	1/28/2004 2:03:43 PM
w-northon-lt3.grassval...	Profile XP	Fan OK	1/28/2004 2:03:43 PM

System Name	w-northon-lt3.grassvalleygroup.com		
IP Address	10.16.38.42	Received Time	1/28/2004 2:03:43 PM
Subsystem	Fans	Facility	Profile XP
Description	One or more system cooling-fans have failed or the fan assembly has been removed. Replace the fan assembly.		
Remarks	Waiting for part to arrive		
			Save

3. Click **Save** to save your text.

Copying messages

You can copy the text of a NetCentral message onto the Windows clipboard. This allows you to paste the message into a document or application for communication and record keeping outside of NetCentral.

When you copy the message, NetCentral places information about the message on the Windows clipboard, as in the following example:

```
Event Alias: Fan Fault
Date: Wednesday, January 28, 2004
Time: 2:03:43 PM
Device: w-northon-lt3.grassvalleygroup.com
Subsystem: Fans
Severity: 2
Description: One or more system cooling-fans have
failed or the fan assembly has been removed.
Replace the fan assembly.
Remarks: Waiting for part to arrive
```

To copy a message, right-click the message and select **Copy**.

Configuring actions and notifications

You can configure the NetCentral system to trigger one or more actions whenever it receives a message or whenever a NetCentral system event occurs. For each action that is triggered, you can also set unique properties. In this way you can trigger the same type of action multiple times, but set the properties differently for each action. This is useful for multiple notifications, such as sending e-mail to several different addresses. By configuring actions in this way you can create many sets of customized notifications.

The following topics describe how to use NetCentral actions:

- [“Adding and modifying actions” on page 87](#)
- [“Setting default action settings” on page 91](#)
- [“Sending e-mail and pager notifications” on page 91](#)
- [“Playing a sound file” on page 94](#)
- [“Playing a beep” on page 95](#)
- [“Running a program” on page 96](#)
- [“Launching a URL” on page 98](#)
- [“Using other actions” on page 99](#)

The actions detailed in this section are those available by default with NetCentral manager software. Other device-specific actions might be available for certain devices or products, as explained in [“Using other actions” on page 99](#).

Adding and modifying actions

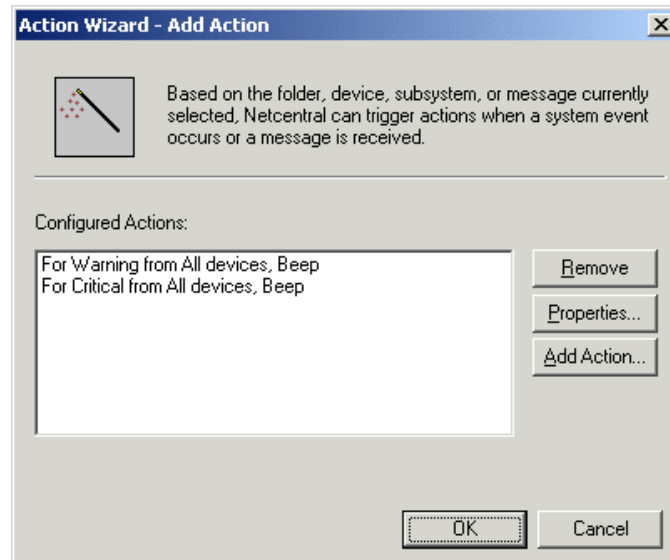
Actions are configured using the Actions wizard. Since the properties are different for each type of action, they may require some special preparations, such as procuring a sound file or a program. Read the explanation for each type of action to determine if you need to do some preparations before you can add a particular action.

Adding actions for devices

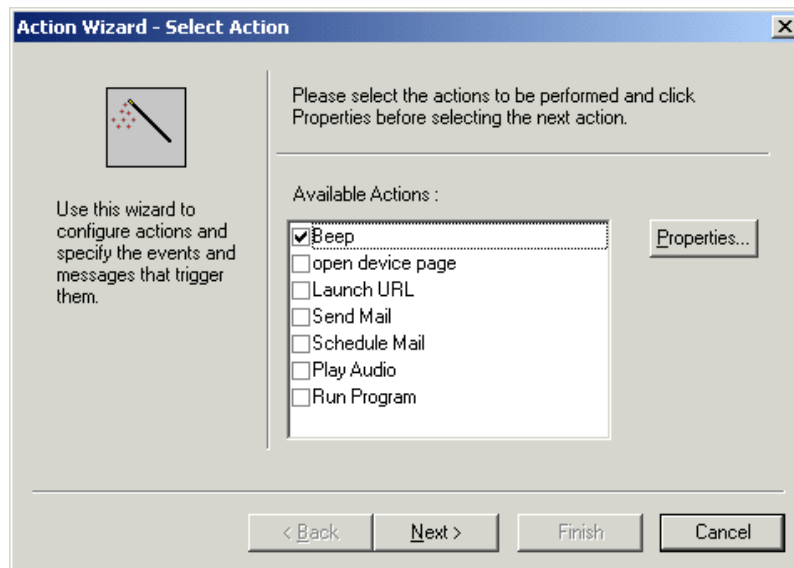
To add an action for messages from a device, device-type, group of devices, or all devices, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click the **Actions** view control button.
3. In the Tree view select a device that corresponds to the action you want to configure.

4. Click **Actions** | **Add Actions**. You can also right-click and select **Add Actions**. The Action Wizard - Add Action dialog box opens.



5. Click **Add Action**. The Select Action screen appears.



6. Follow the wizard instructions and configure your action or actions.
To configure action properties, refer to the procedure later in this section for the specific action.
7. Click **Finish** when you are done with the wizard. Your new action appears in the main Actions view.

8. Continue to add actions as required.
 9. In the Actions view, select folders, devices, and subsystems in the Tree view hierarchy to display and verify currently configured actions.
- Actions “ripple up” through the hierarchy so that parent nodes display their own actions as well as those of their children nodes. When the top-level **Monitored Devices** folder is selected, all action are displayed.

Adding an action for a folder

If you want to receive a special notification from NetCentral when a message is received from any device in a particular folder, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. In the Tree view, right-click the folder and select **Add Actions**. The Actions wizard opens.
3. Follow the wizard instructions and configure your action. Since you are adding an action for a folder, the wizard restricts your configurations as appropriate for the folder. Click **Finish** when you are done with the wizard.

Adding an action for a subsystem

If you want to receive a special notification from NetCentral when a message is received from a particular subsystem of a device, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. In the Tree view, right-click the subsystem and select **Add Actions**. The Actions wizard opens.
3. Follow the wizard instructions and configure your action. Since you are adding an action for a subsystem, the wizard restricts your configurations as appropriate for the subsystem. Click **Finish** when you are done with the wizard.

Adding an action for a message

You might want to receive a special notification from NetCentral when a particular message is received from a specific device. For example, if a device sends a message indicating a problem and you are working on the problem, you might want to run tests and be notified immediately if the problem occurs again. You can use the previous procedure [“Adding actions for devices”](#) to configure this type of action. However, if the device has recently received the message in which you are interested, the following procedure offers a more direct method.

To add an action for a recently received message from a device, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click the **Messages** view control button
3. In the Tree view select the device. Messages appear in the Information area.
4. Right-click the message in which you are interested and select **Add Actions**. The Actions wizard opens.
5. Follow the wizard instructions and configure your action. Since you are adding an

action for a specific message, the wizard restricts your configurations as appropriate for the message. Click **Finish** when you are done with the wizard.

6. Click the **Actions** view control button and select folders, devices, and subsystems to verify the actions currently configured.

Modifying or removing an action

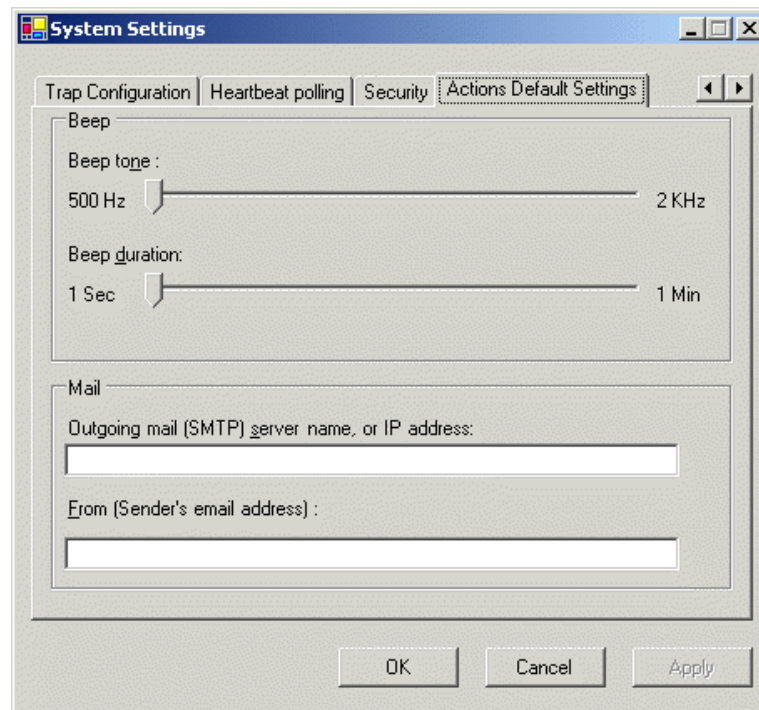
To modify or remove an action, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click the **Actions** View control button.
3. Select the folder, device, or subsystem to which the action you want to remove or modify is configured. For best results select the top-most point in the Tree view hierarchy to which the actions is configured. For example, if the action is configured for all the devices in a folder, select the folder rather than one of the devices in the folder. This simplifies the process of modifying an action.
4. In the Information area, right-click the action.
5. To remove the action select **Delete**.
If an action is configured for all devices and you remove it as it is listed for any single device, the action is removed for all devices.
6. To modify the action select **Properties** or **Add Action | Properties**.
7. Re-configure the action.
8. Click the **Actions** view control button and select folders, devices, and subsystems to verify the actions currently configured.

Setting default action settings

You can set default values for the properties of Mail actions and Beep actions as follows:

1. Click **Configure | Global Action Configuration**. The Device Configuration dialog box opens with the Actions Default Settings tab selected.



2. Configure properties for the Beep action. Refer to [“Playing a beep” on page 95](#). When you add a Beep action in the future, its properties will be pre-configured by default with these settings.
3. Configure properties for the Mail action. Refer to [“Sending e-mail and pager notifications” on page 91](#). When you add a Mail action in the future, its properties will be pre-configured by default with these settings.
4. Click **OK** to save settings and close.

Sending e-mail and pager notifications

You have two different actions available to you for sending e-mail, as follows:

Send Mail — Sends unscheduled e-mail to the recipients that you specify, regardless of the day or time.

Schedule Mail — Sends scheduled e-mail to the recipients that you specify according to the days and times that you configure. For both of these e-mail actions, the NetCentral system sends the full text of the NetCentral message as e-mail to the address that you specify. In order to configure properties and add either of these actions, prepare the following information:

- The Simple Mail Transfer Protocol (SMTP) server name or IP address for the server that will send e-mail *from* the NetCentral server. Do not confuse this with IP addresses used for SNMP trap destination configuration elsewhere to send SNMP messages *to* the NetCentral server.
- The e-mail address to which you want to send the message.
- The e-mail address that you want to appear on the “From” line of the e-mail sent from the NetCentral system.

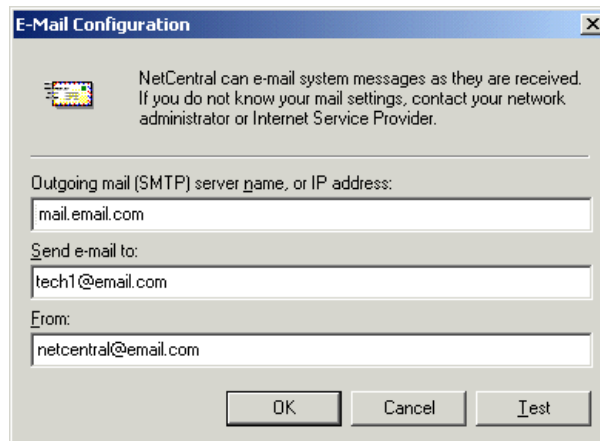
You can also use these actions to notify a pager or cell phone if the pager or cell phone service is able to accept e-mail messages. One example of an address to which you might send an e-mail is (501)234-5678@mobil.telco.net. Remember that many pager systems limit the number of characters allowed in a message, so not all of the alarm message would be transmitted if it exceeds that number.

To configure default settings for Mail actions, refer to [“Setting default action settings” on page 91](#)

Configuring properties for sending unscheduled e-mail

To configure properties for sending unscheduled e-mail, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. As explained in [“Adding and modifying actions” on page 87](#), open the Actions wizard, add or modify a rule for this action and click **Properties**. The E-mail Configuration dialog box appears.



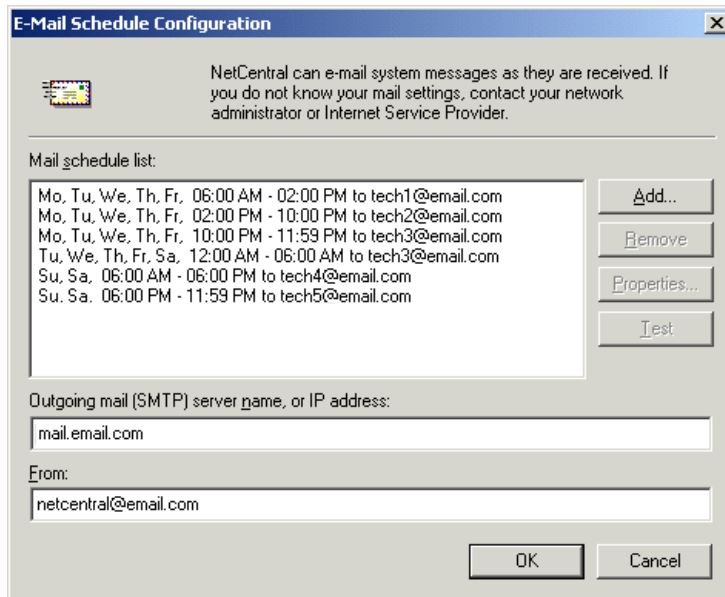
3. As indicated by the interface text, enter the e-mail and server address information.
4. Click the **Test** button to send a test message to the recipient. A message box will be displayed to report the results of the e-mail test.
5. When you are satisfied with your settings, click the **OK** button to close the dialog box and save your settings.

Configuring properties for sending scheduled e-mail

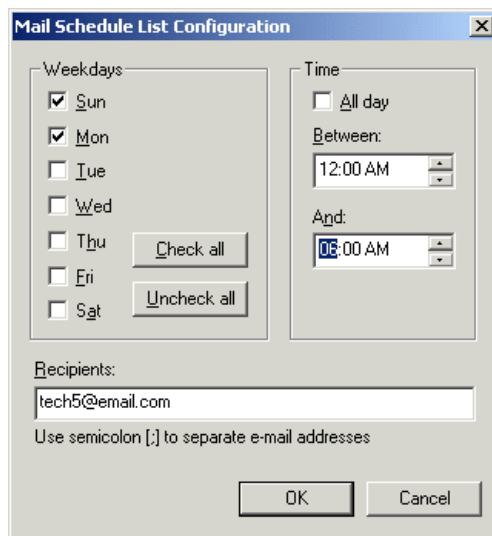
To configure properties for sending scheduled e-mail, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.

2. As explained in [“Adding and modifying actions” on page 87](#), open the Actions wizard, add or modify a rule for this action and click **Properties**. The E-mail Schedule Configuration dialog box appears.



3. As indicated by the interface text, enter the e-mail and server address information.
4. Click the **Add** button. The Mail Schedule List Configuration dialog box opens.



5. In the Recipients box, enter the e-mail addresses of the persons to whom you want to send e-mail.
6. Check the days of the week on which you want e-mail sent to your recipients.
7. Configure the time of the day during which you want e-mail sent to your recipients. For time periods that span midnight, configure two dialog boxes, one for the time

period ending at 11:59 P.M. and another for the time period starting at 12:00 A.M. on the next day.

8. When you are satisfied with your settings, click the **OK** button to close the dialog box. Your schedule appears in the Mail schedule list on the E-mail Schedule Configuration dialog box.
9. Continue to add, remove, or modify properties to create your desired list of mail schedules. Select a schedule from the list and use the **Test** button to verify your e-mail configurations.
10. When you are done, click the **OK** button to save the mail schedules and close the E-mail Schedule Configuration dialog box.

Playing a sound file

When you add the Play audio action, the NetCentral manager software automatically plays the sounds contained in the Wave file you specify. A Wave file is a standard audio file format identified by a file name extension of WAV (.wav). You can set the NetCentral manager software to play the Wave file from 1 to 1000 times.

In order to configure properties and add this action, you will need to make the following preparations:

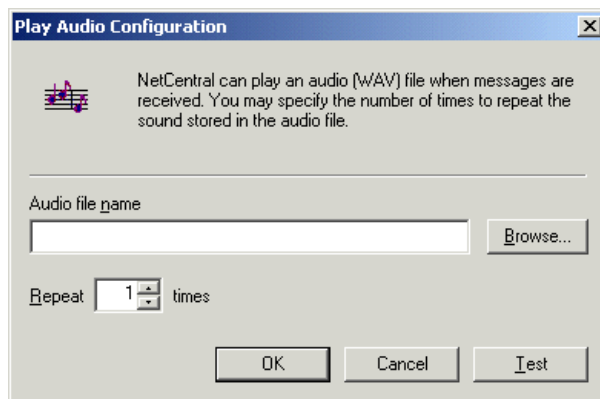
- Procure or create the Wave file.
- Place the Wave file in a location on the NetCentral server PC.
- Copy the Wave file to each of your NetCentral client PCs so that it is in the same location on each of the NetCentral client PCs as it is on the NetCentral server PC. Alternatively, you can place the Wave file in a common location accessible to both the NetCentral server PC and all NetCentral client PCs
- Make note of the location and name of the Wave file.

Your PC must have a sound card and speaker in order to make the sound audible.

Configuring properties for playing an audio file

To configure properties for playing an audio file, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. As explained in [“Adding and modifying actions” on page 87](#), open the Actions wizard, add or modify a rule for this action and click **Properties**. The Play Audio Configuration dialog box appears.



3. As indicated by the interface text, enter the full path and name of the Wave file, or click **Browse** and navigate to the file using the Open dialog box.
4. In the Repeat box, select the number of times that you want the NetCentral manager software to play the Wave file each time it performs this action.
5. Click the **Test** button to hear a test of the audio file.
6. When you are satisfied with your settings, click the **OK** button to close the dialog box and save your settings.

Playing a beep

When you add the Beep action, the NetCentral manager software automatically plays a beep on the PC. By setting the tone and duration of the beep you can create audible alerts that are distinguishable from one another.

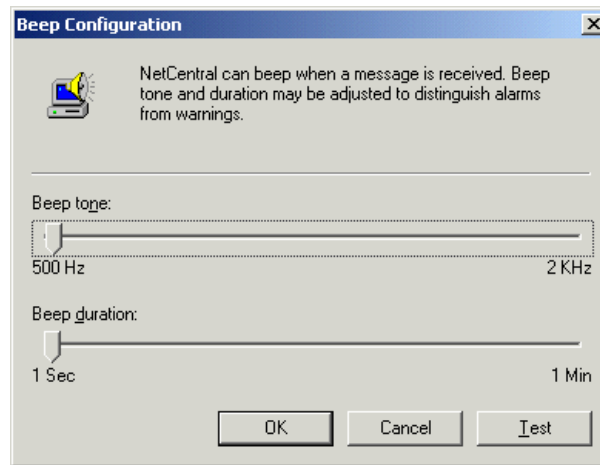
In order to configure properties and add this action, you do not need to make any special preparations, since the NetCentral manager software uses the PC's built-in beep sound.

To configure default settings for Beep actions, refer to [“Setting default action settings” on page 91](#)

Configuring properties for playing a beep

To configure properties for playing a beep, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. As explained in [“Adding and modifying actions” on page 87](#), open the Actions wizard, add or modify a rule for this action and click **Properties**. The Beep Configuration dialog box appears.



3. Adjust the sliders for tone and duration to create an identifiable sound.
4. Click the **Test** button to hear a test of the sound that you have created.
5. When you are satisfied with your settings, click the **OK** button to close the dialog box and save your settings.

Running a program

When you add the Run Program action, the NetCentral manager software automatically executes a program of your choice.

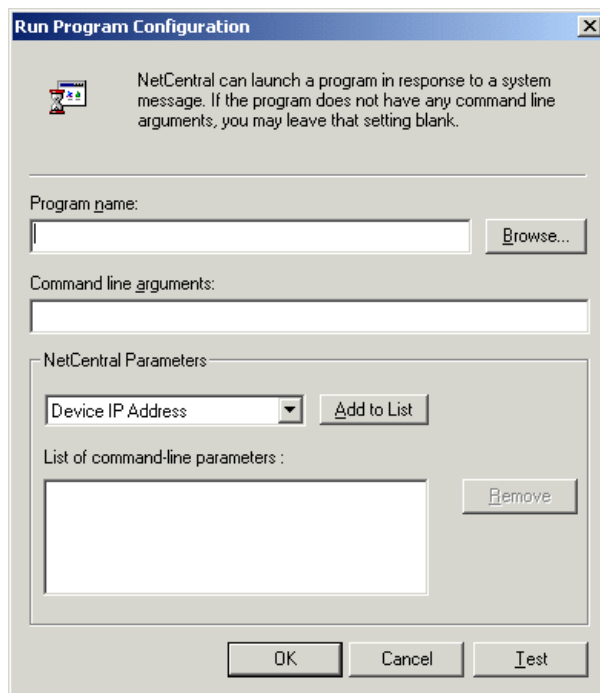
In order to configure properties and add this action, you will need make the following preparations:

- Procure or create your program. The program must be Win32 executable.
- Make note of command line arguments (if any) that you want the NetCentral manager software to pass to your program.
- Place the program file or files in a location on the NetCentral server PC.
- Copy the program file or files to each of your NetCentral client PCs so that it is in the same location on each of the NetCentral client PCs as it is on the NetCentral server PC. Alternatively, you can place the program file or files in a common location accessible to both the NetCentral server PC and all NetCentral client PCs
- Make note of the location and name of your program.

Configuring properties for running a program

To configure properties for running a program, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. As explained in [“Adding and modifying actions” on page 87](#), open the Actions wizard, add or modify a rule for this action and click **Properties**. The Run Program Configuration dialog box appears.



3. As indicated by the interface text, enter the full path and name of your program, or click **Browse** and navigate to your program using the Open dialog box.
4. In the Command line arguments box enter any arguments that you want the NetCentral manager software to pass to your program.
5. To insert a NetCentral parameter into your command line, select the NetCentral parameter that you want to add to your command line and click **Add to List**. When an action is fired, NetCentral parameters are placed after the command line parameters, as illustrated by the following example:

The program is *C:\Winnt\Sample.exe*, your command line arguments are “arg1 arg2” (two arguments), and you choose “Device IPAddress” as your NetCentral parameter. If a message comes from a device with IP address 10.255.104.188 that triggers the action, program *Sample.exe* is fired with arguments as follows:

```
arg1 arg2 10.255.104.188
```

As you can see, NetCentral appends just the value of fields and not the parameter name, Value pair. Compile a list of all the parameters you want.

6. Click the **Test** button to execute your program in test mode, without parameters appended to the command line. To test a parameter, you must cause an actual fault on the device to trigger the appropriate SNMP trap message, as the configured parameters will be appended to the command line arguments only when an actual firing on a fault happens.
7. When you are satisfied with your settings, click the **OK** button to close the dialog box and save your settings.

Launching a URL

When you add the Launch URL action, the NetCentral manager software automatically opens your default Web browser and points it to a URL of your choice. You can also configure this action so that it adds NetCentral values, based on the message that triggers the action, into the URL. Parameters configured in this way are intended for use with an Active Server Page (ASP) script.

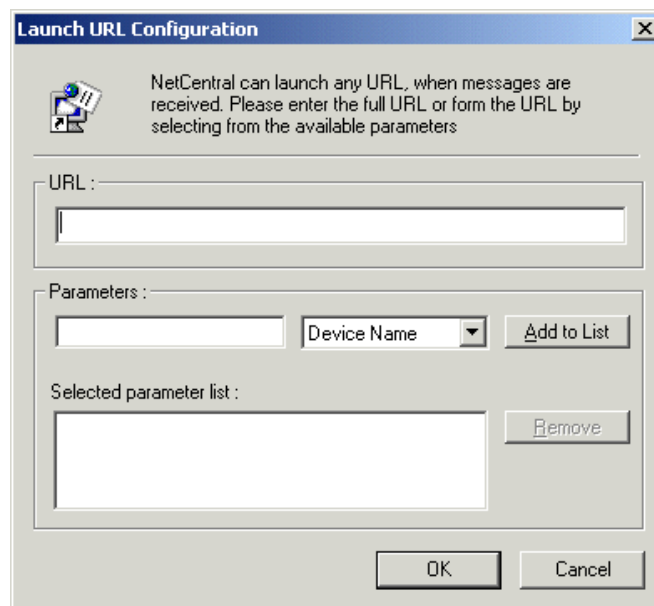
In order to configure properties and add this action, you will need make the following preparations:

- Setup, create, or find the Web site for this action. Make sure that the Web site is accessible from the NetCentral server PC as well as from all NetCentral client PCs.
- Note the URL for the Web site
- If using parameters, create the ASP script for the parameters

Configuring properties for launching a URL

To configure properties for launching a URL, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. As explained in [“Adding and modifying actions” on page 87](#), open the Actions wizard, add or modify a rule for this action and click **Properties**. The Launch URL Configuration dialog box appears.



3. Enter the URL to which you want your Web browser pointed.
4. If desired, define NetCentral parameters that you want to add to the URL. When the URL is launched, any parameters you have defined are placed after the URL so that they can be passed to an ASP script, as illustrated by the following example:

The URL is *http://www.company.asp*. One parameter is defined as “name” for “Device Name”, another parameter is defined as “ip” for “Device IPAddress”.

If a message comes from a device named xp1 with IP address 10.255.104.188 and the message triggers this action, the following URL is launched:

`http://www.company.asp?name=xp1&ip=10.255.104.188`

As you can see, the URL is appended with a question mark (?) first and then parameter name - value pairs each separated by the “and” symbol (&).

5. As you define parameters, click **Add to List** or **Remove** to create your list of parameters.
6. When you are satisfied with your settings, click the **OK** button to close the dialog box and save your settings.

Using other actions

As you explore the Actions wizard, you might notice actions in the list that are not described in this manual. These other actions are on the list for the following reasons:

- Different device-types can have their own action providers that plug-in to the NetCentral manager software, as explained in [“Action providers” on page 19](#). These actions become available when the device provider software is installed. Read the documentation for the devices monitored by your NetCentral system for information about their actions.
- You have created one or more Named Actions in a previous use of the Actions Wizard. A Named Action is an action or a group of actions that you have configured and then assigned a unique name. NetCentral retains Named Actions with their configurations and puts them on the list of actions so that you can use them again. However, if a Named Action contains more than one configured action, the Actions Wizard does not allow it to then be combined with yet more configured actions to create a new Named Action. This would create a double nested action, which is not allowed.

Filtering messages to disable actions

If you find that certain messages are not necessary, you can have the NetCentral system selectively filter these messages so that no action is triggered when the message is received. For example, if a project requires frequent changes in the timing parameters on one of your Profile XP Media Platforms, you might not want to have actions repeatedly triggered for the “System timing out of sync” message from that Profile XP Media Platform. In this case you can have the NetCentral system filter the message from that Profile XP Media Platform only, yet continue to monitor for other messages.

When a message is filtered, the NetCentral system disables the currently configured actions for that message and does not display the message or any of its status indicators in the Messages view. Instead, the filtered message is diverted to the Actions view, where you can view a list of filtered messages in the bottom pane of the information area.

The following sections provide procedures for filtering messages:

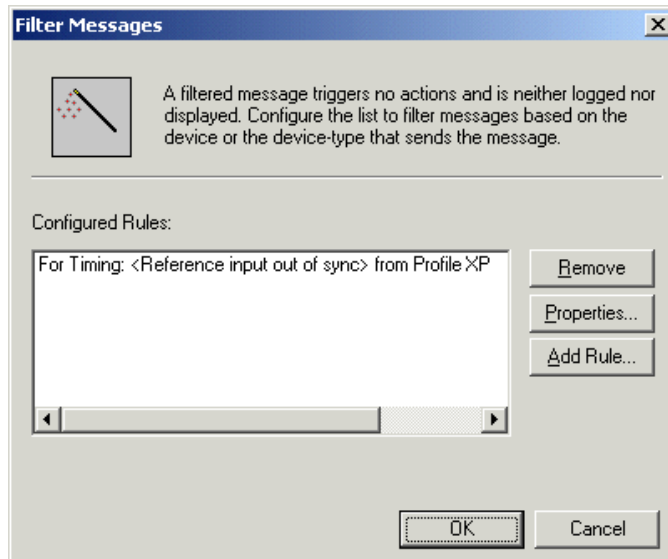
- [“Filtering messages by device” on page 100](#)
- [“Filtering messages by folder” on page 101](#)
- [“Filtering messages by subsystem” on page 102](#)
- [“Filtering a displayed message” on page 102](#)

Filtering messages by device

This procedure allows you to filter select messages based on the device or device-type from which the messages come.

To filter messages by device, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. In the Tree view, right-click the device or device-type from which you want a message filtered and select **Filter Messages**. The Filter Message dialog box opens.



3. Select **Add Rule**. The Filter Message wizard opens.
4. Follow the wizard instructions and configure a rule to filter a message or messages. Click **Finish** when you are done with the wizard. Your new rule appears in the Filter Message dialog box.
5. If you are filtering more than one specific message, repeat this procedure to compile a list of messages that you want filter, using the Add Rule button and the Remove button. As you add messages, the wizard will disable the messages already added to help you avoid conflicts in the rules you are configuring.

NOTE: Take care as you add multiple filter message rules that you do not create conflicting rules that cancel out one another.

6. When you are satisfied with your settings, click the **OK** button to put the settings into effect and close the Filter Message dialog box.

Filtering messages by folder

This procedure allows you to filter messages based on a selected folder in the Tree view so that all messages from all devices in the selected folder are filtered. For example, if you set up a “Maintenance” folder in this way, you can move devices into the folder whenever you are servicing them and easily eliminate the multiple alarm notifications that your service work might generate. If you use this technique for devices represented by graphical view active drawings, you should also edit the HTML page, as explained in [“Creating a Facility graphical view” on page 57](#).

To filter messages by folder, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. In the Tree view, right-click the folder that contains the devices from which you want all messages filter and select **Filter Actions**. The Filter Messages dialog box opens.
3. Select **Add Rule**. The Filter Message wizard opens.

4. Follow the wizard instructions and configure a rule to filter messages for the folder. Since you are filtering messages for a folder, the wizard restricts your configurations as appropriate for the folder. Click **Finish** when you are done with the wizard. Your new rule appears in the Filter Message dialog box.

Filtering messages by subsystem

This procedure allows you to filter messages based on a subsystem of a device, as selected in the Tree view, so that all messages from the subsystem are filtered.

To filter messages by subsystem, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. In the Tree view, right-click the subsystem and select **Filter Actions**. The Filter Messages dialog box opens.
3. Select **Add Rule**. The Filter Message wizard opens.
4. Follow the wizard instructions and configure a rule to filter messages for the subsystem. Since you are filtering messages for a subsystem, the wizard restricts your configurations as appropriate for the subsystem. Click **Finish** when you are done with the wizard. Your new rule appears in the Filter Message dialog box.

Filtering a displayed message

If a message is currently displayed in the Messages view, the following procedure offers a direct method to filter that message only.

To filter a displayed message, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click the **Messages** View control button and select the device that has the message that you want to filter. Messages appear in the Messages view area.
3. Right-click the message you want to filter and select **Filter Message**. The Filter Messages dialog box opens.
4. Select **Add Rule**. The Filter Message wizard opens.
5. Follow the wizard instructions and configure a rule to filter the message. Since you are filtering a specific message, the wizard restricts your configurations as appropriate. Click **Finish** when you are done with the wizard. Your new rule appears in the Filter Message dialog box.

Administering the NetCentral system

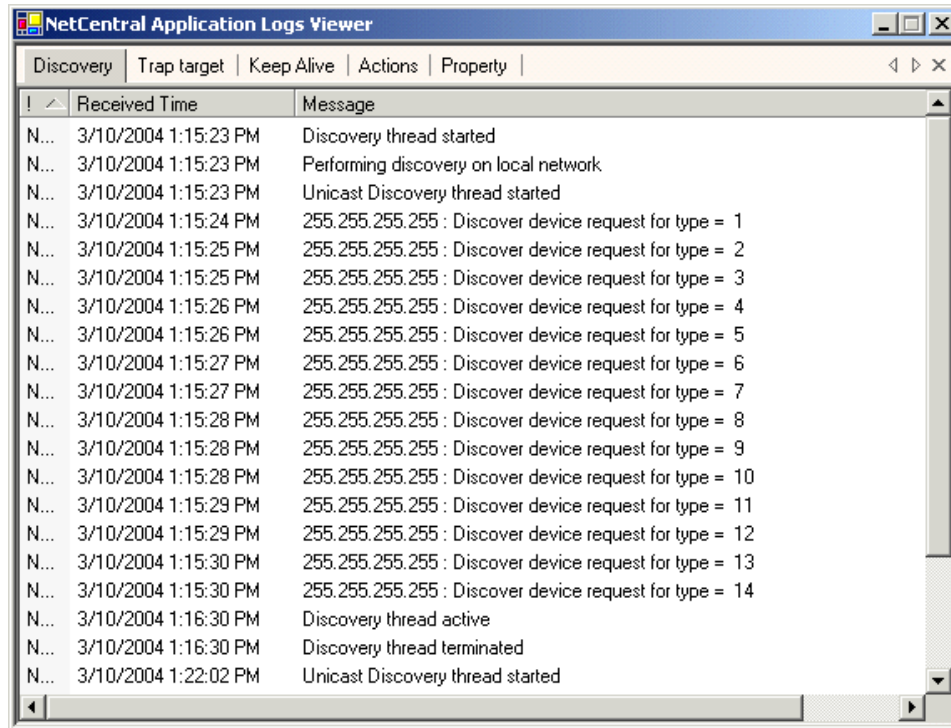
This section provides administrative procedures for the NetCentral system. Topics are as follows:

- [“Using the Application Logs Viewer” on page 104](#)
- [“Adding devices” on page 104](#)
- [“Removing devices” on page 108](#)
- [“Setting automatic SNMP trap configuration” on page 109](#)
- [“Setting heartbeat polling” on page 111](#)
- [“Managing NetCentral security” on page 113](#)
- [“Backing up the NetCentral database” on page 117](#)
- [“Accommodating NetCentral database growth” on page 118](#)
- [“Setting up for remote access” on page 118](#)
- [“Verifying components installed and running” on page 118](#)
- [“Connecting a NetCentral client to a different NetCentral server” on page 120](#)
- [“Adding custom tools” on page 120](#)

Using the Application Logs Viewer

NetCentral reports all its automatic processes to the Application Logs Viewer. Click **Logs | Application Logs** to open the Application Logs Viewer. Then click the tab for the type of automatic process in which you are interested.

Also refer to [“About logs that contain NetCentral system information” on page 128](#).



Adding devices

This section provides procedures for controlling how and when devices are added to the NetCentral system for monitoring. Topics include the following:

- [“About the discovery process” on page 104](#)
- [“Manually adding a device” on page 105](#)
- [“Configuring Auto-discovery to add devices” on page 106](#)

About the discovery process

Whenever a device is added, whether automatically or manually, the NetCentral system executes the discovery process. The discovery process finds the device, gathers information about the device, and then triggers the SNMP trap configuration process, which attempts to remotely configure SNMP trap destinations on the device so that it sends its SNMP trap messages to the NetCentral server PC. These processes are reported in the Application Logs Viewer. Also, the appearance of the device in the

NetCentral window indicates the results of these processes, as explained in [“Verify SNMP trap messages from monitored devices” on page 38](#). Refer to [“Setting automatic SNMP trap configuration” on page 109](#) for more information.

You direct the software to use the discovery process when you manually add a single device. You can also configure the way the software runs this process in “Auto-Discovery” mode. Once a device has been added to the NetCentral system, the software remembers it and tries to “discover” that device every time it starts.

When you add devices, you are giving directions to the discovery process as it looks for devices to add. You specify these directions by entering the following information about the device or devices that you want to add:

- **SNMP Community name** — Each device must belong to one or more SNMP communities. Typically, you would make each device a member of the “public” community so that all devices can send messages to NetCentral servers. You can optionally create and configure other SNMP community names if you want to restrict messages by community.
- **IP address or Name** — Each device must have an Internet Protocol (IP) address in order to be a part of an IP network. Use these IP addresses to identify the devices that you want to add to the NetCentral system. Alternatively, if your network recognizes names, you can add devices one at a time by entering the network name of the device. Contact your network administrator for information regarding the names or IP addresses of your monitored devices.

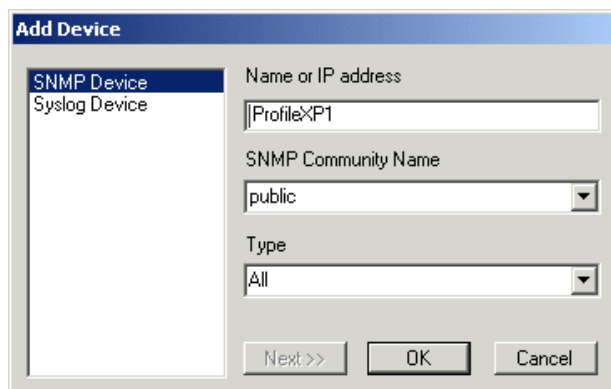
Manually adding a device

When you manually add a SNMP-monitored device, NetCentral uses the same discovery process it uses in Auto-discovery, except it targets only the device you are adding.

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 42](#).

To manually add a SNMP-monitored device, do the following:

1. Make sure you are logged on to NetCentral with administrator-level privileges.
2. Click **File | Add | Device**. The Add Device dialog box opens.



3. Select **SNMP Device**.
4. Enter the name or IP address of the device you want to add.

5. Enter `public` as the SNMP community name. This is the default SNMP community name pre-configured on most devices. You can enter another community name if you have a specialized SNMP environment that uses unique community names. In any case the device must have a SNMP community name in order to add the device to NetCentral. If the device has no SNMP community name, you must first configure one on the device before proceeding, as explained in [“Set SNMP trap destinations on monitored devices” on page 39](#). Devices with no community name cannot be added.
6. To make the discovery process more efficient, on the **Type** drop-down list you can select the type of device. If the device-type you want to monitor is not on the list, it means the device provider is not installed.
7. Click the **OK** button to close the dialog box.

A “Network Connection” message box appears while NetCentral runs the discovery process and attempts to set a SNMP trap destination on the device. NetCentral reports these processes in the Application Logs Viewer. If NetCentral cannot add the device, an informative message is displayed. As advised by the message, check network connectivity, SNMP community name, and make sure the device is NetCentral compatible, then repeat this procedure.

A successfully added device appears in the Tree view.
8. Check the Application Log for SNMP trap configuration messages for the device. If SNMP trap configuration was not successful, accomplish additional steps, as explained in [“Verify SNMP trap messages from monitored devices” on page 38](#).

Configuring Auto-discovery to add devices

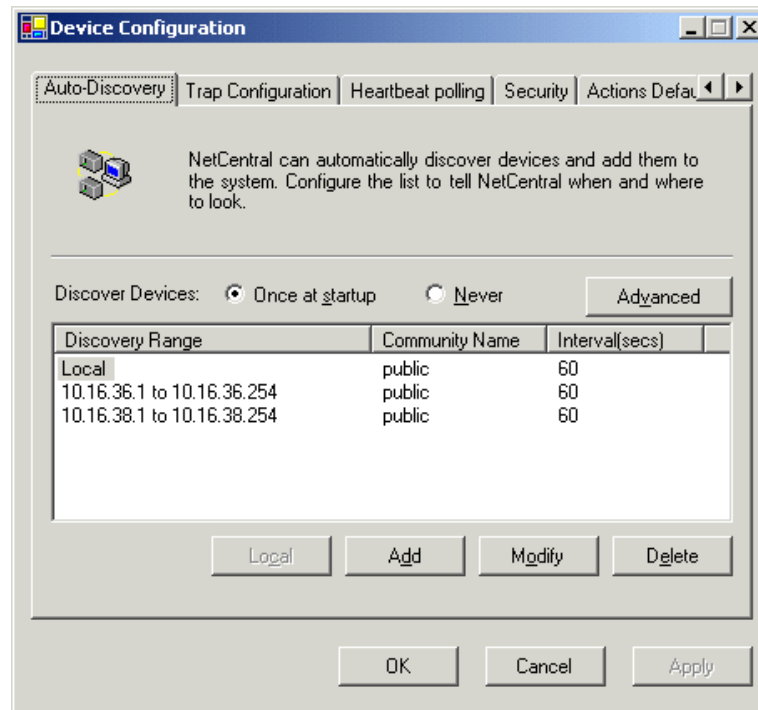
By default at startup Auto-discovery adds all the NetCentral-compatible SNMP-monitored devices it finds on the local network to your NetCentral system. This section explains how to change the default Auto-discovery settings so that when Auto-discovery runs it more reliably and efficiently keeps those devices that you want to monitor added to your system, even if you frequently add or remove devices in your facility.

NetCentral reports Auto-discovery processes in the Application Log.

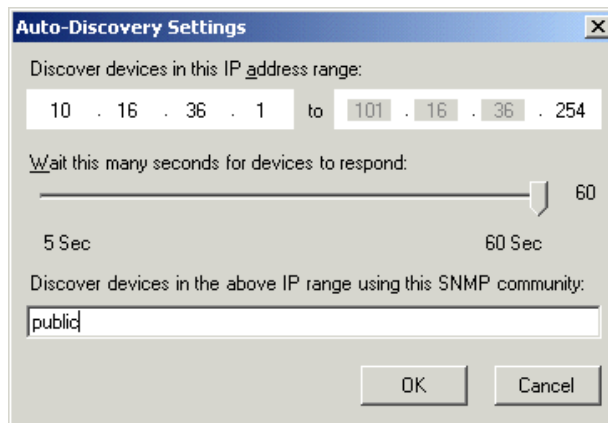
For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 42](#).

To configure Auto-Discovery, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click **Configure | Auto Discovery**. When the System Settings dialog box opens, click the **Auto-Discovery** tab.



- By default, Auto-Discovery discovers devices at application start on the local network only. To configure Auto-Discovery to run in other networks, click the **Add** button. The Auto-Discovery Settings dialog box opens.



- Specify the IP address range on the network within which you want NetCentral to search for devices and enter the SNMP community name to which the devices belong. Typically, you would set the community name to "public". Contact your network administrator for specifics on IP addresses for your network.
- Adjust the slider to regulate the amount of time that NetCentral waits for a device to respond in order to be discovered. If the network that you are searching is prone to lengthy connection times, such as across a Wide Area Network in a geographically distant location, adjust the slider to allow more time for a device to

respond.

6. When you are satisfied with your settings, click the **OK** button to close the Auto-Discovery dialog box.
7. Choose the **Discover Devices** option that gives you the Auto-Discovery timing that you need, as follows:
 - **Never** — The Auto-Discovery process is turned off all together. Selecting this option over-rides previously configured Advanced settings.
 - **Once at startup** — The Auto-Discovery process runs only when the NetCentral manager software starts up. Selecting this option over-rides previously configured Advanced settings.
 - **Advanced** — Clicking this button opens a dialog box in which you can configure the days and times during which you want the NetCentral system to run Auto-Discovery. This is especially useful if you frequently have NetCentral compatible devices added to your network. To minimize the impact on system and network performance, schedule Auto-Discovery to run during times of minimal activity.

NOTE: *Once your Advanced schedule is set, do not then select “Once at startup” or “Never”, as these options over-ride the Advanced schedule.*

If you configure an extensive range of IP addresses within which the Auto-Discovery process runs, you may find the process creates a noticeable load on your PC system resources. If this is the case, after you have initially discovered all your monitored devices, you can select **Never** and subsequently use Auto-Discovery only when needed.

8. Continue to configure the list so that NetCentral runs Auto-Discovery as desired. Use the Modify and Delete buttons as necessary to create your Auto-Discovery list. If you delete the default Local network, you can restore it with Local button.
9. When you are satisfied with the list, click the **Apply** button, then the **OK** button to close the System Settings dialog box.
10. Click **Configure | Stop Auto-discovery**, then click **Configure | Start Auto-discovery**. If the Configure menu reports *Stopping...*, wait until it changes to *Start* This puts your changes into effect.

Removing devices

When you remove a device, it disappears from the NetCentral window and the NetCentral server software ceases to process the messages that come from the device.

To remove a device, do the following:

1. Make sure you are logged in to NetCentral with administrator-level privileges.
2. In the Tree view, highlight the device you want to remove.
3. Right-click the device or click **File** and select **Remove**. You can also press **Delete**. The Delete Device message box appears, asking “...do you really want to delete...?”.

4. Click the **Yes** button to remove the device and close the message box.
5. Repeat this procedure as necessary until all undesired devices are removed.
6. If a removed device is represented on a Facility view HTML page, you must manually remove it from the HTML page as well.
7. If you find that a removed device re-appears at a later time, it means that the Auto-discovery process is discovering and re-adding the device.

The Auto-Discovery process will discover and add devices in the configured IP range, including devices that you have previously removed. If you want to keep a removed device from being added to the system again every time Auto-Discovery runs, reconfigure your Auto-Discovery ranges to exclude the IP address of the removed device. For example, if a device that you want to keep removed has an IP address of 192.168.6.155, configure two Auto-Discovery Settings dialog boxes, one to run through the IP addresses below 192.168.6.155 and another to run through the IP addresses above 192.168.6.155.

Setting automatic SNMP trap configuration

By default at startup and whenever a device is added, NetCentral manager software automatically runs a remote SNMP trap configuration process in an attempt to make sure that all devices have their SNMP trap messages correctly enabled. This section explains how you can change the timing of when the remote trap configuration runs so that it can respond more effectively to changes in your system environment.

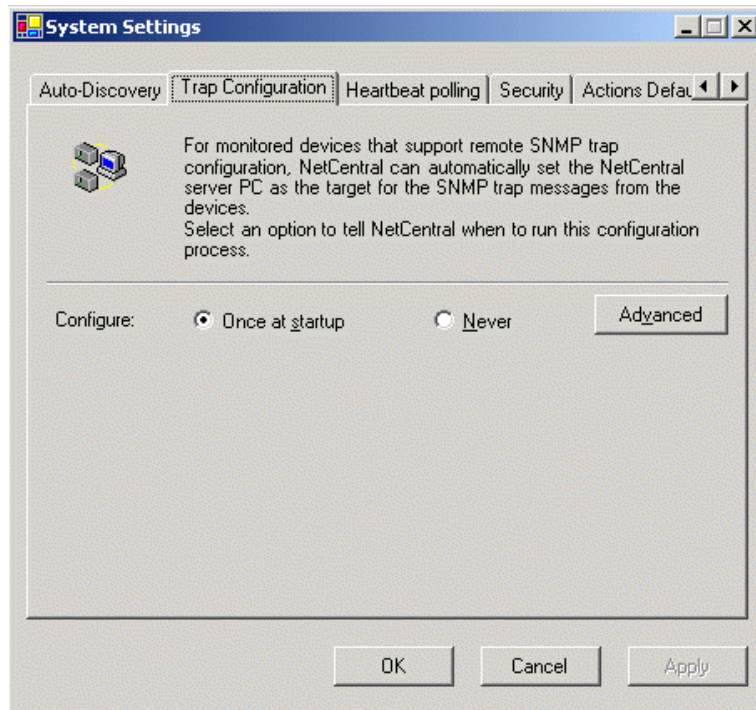
The purpose of the SNMP trap configuration process is to ensure that all devices have the IP address of the NetCentral server PC entered as a SNMP trap destination. The process runs in the following phases. These phases are reported in the Application Logs Viewer:

1. Test phase — NetCentral tests each monitored device to determine if it is able to send its SNMP trap messages to the NetCentral server. When trap configuration is automatically run in conjunction with a device being added, this test is always run after the discovery process, so any newly discovered and added devices are immediately tested.
2. Test report phase — NetCentral reports the results of the test phase in the Application Logs Viewer. Also, regardless of how you configure the overall SNMP trap configuration process to run, these first two phases (Test and Test report) always run when NetCentral starts up.
3. Configuration phase — If the device is not able to send a SNMP trap message, NetCentral determines whether or not that type of device supports remote trap configuration. If it does, NetCentral attempts to remotely configure the trap destination on the device and enter the IP address of the NetCentral server.
4. Configuration report phase — NetCentral reports the results of the configuration processes in the Application Logs Viewer.

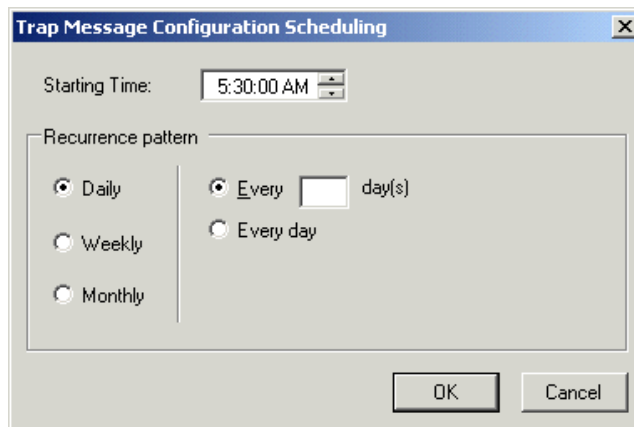
As explained in the following sections, you can configure the way the NetCentral manager software automatically configures trap destinations. You can also manually use NetCentral's remote trap configuration, as explained in [“Verify SNMP trap messages from monitored devices” on page 38](#). Choose the methods that are appropriate for your particular environment.

To modify settings for automatic SNMP trap configuration, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click **Configure | Trap Configuration**. When the System Settings dialog box opens, click the **Trap Configuration** tab.



3. By default the process runs automatically on all devices only at application start. After that, as long as your NetCentral manager software continues to run, trap configuration remains in a stand-by mode. When a device is added, trap configuration is executed for that device only. In this mode it does not consume significant network bandwidth, so in most cases there is no need to turn it off. However, if you want to turn off trap configuration permanently, click **Never** and **OK** to save settings and close.
4. If you want to change the timing at which trap configuration automatically runs on all devices, click **Advanced**. The Trap Message Configuration Scheduling dialog box opens.



5. Configure the settings according to the days and times that you want the process to run. To minimize the impact on system and network performance, schedule the process to run during times of minimal activity. If you schedule the process to run at a regular interval in this way, NetCentral updates the SNMP trap configuration reports in the Application Logs Viewer for each device as per your schedule, so you can be regularly assured that your devices are capable of sending trap messages.
6. Click **OK** to save settings and close

NOTE: *Once your Advanced schedule is set, do not then select “Once at startup” or “Never”, as these options over-ride the Advanced schedule.*

7. Click **OK** on all the System Settings dialog boxes to save settings and close.
8. Click **Configure | Stop SNMP Trap Message Configuration**, then click **Configure | Start SNMP Trap Message Configuration**. If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts your changes into effect.

Setting heartbeat polling

To make sure that devices are still “alive” and capable of communicating their status, the manager software periodically broadcasts “ping” type messages which request a response from all devices. In this way the NetCentral system does a poll to check the “heartbeat” of devices. If all devices respond, the manager software does not display any messages or trigger any actions. However, if a device does *not* respond, the manager software checks again. If further checks still do not get a response from the device, the device is declared dead or off-line and the NetCentral system triggers critical-level actions to notify you of the condition.

You can configure heartbeat polling by adjusting the following settings:

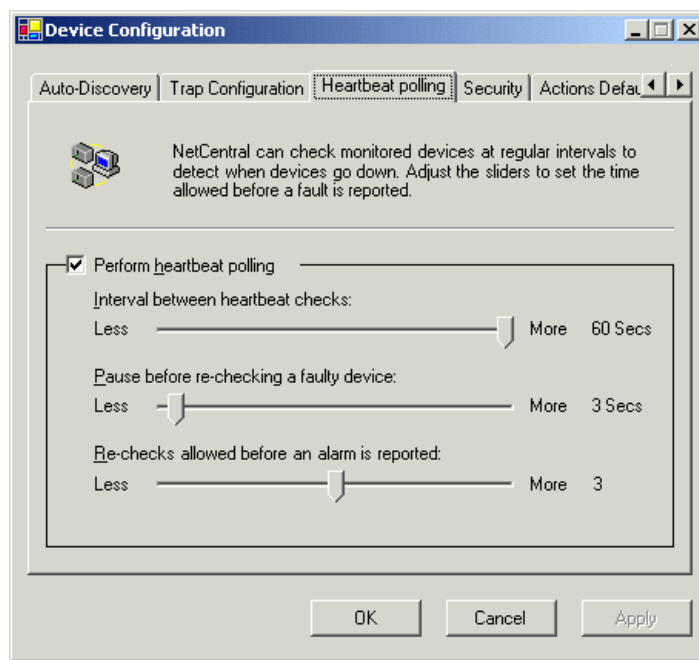
- Interval between heartbeat checks — The period of time that the manager software waits between the routine checks for the heartbeat of all devices.
- Pause before re-checking a faulty device — The period of time that the manager software waits before it re-checks a device that does not respond.
- Re-checks allowed before an alarm is reported — The number of times that the manager software re-checks an unresponsive device before displaying the “Dead or off-line” message and triggering critical-level actions.

When you adjust these settings, you are adjusting the time allowed for a momentary loss of contact before triggering an alarm. For example, if your network commonly experiences minor drop-outs that do not necessarily threaten the health of your devices or systems, you will not want a false alarm every time there is a slight glitch. In this case you would move the sliders to the right to allow more time for a brief lapse in contact to be restored, meaning an alarm would go off only when there is no response from a device for a significant length of time. On the other hand, if your system is highly critical and you need to know immediately of the slightest indication of a problem, you would move the sliders to the left to allow less time, meaning that even a very brief loss of contact would trigger an alarm.

NOTE: *These settings could effect the performance of your network. Settings that cause the polling dialog to occur more frequently increase the amount of network traffic.*

To set heartbeat polling, do the following:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Choose **Configure | Heartbeat Polling**. The System Settings dialog box appears.
3. Click the **Heartbeat Polling** tab.



4. As indicated by the interface text, adjust the sliders to set the time allowance the NetCentral system exercises before it declares a system off-line. Set the “Interval between heartbeat checks” slider so that the NetCentral system checks often enough to give you adequate notification of a problem, but not so often that it unnecessarily increases the traffic on your network. Use similar considerations as you set the other sliders.
5. If you want to temporarily disable the NetCentral system’s heartbeat polling, uncheck the Perform heartbeat polling check-box. Do not disable heartbeat polling

in this way if you are actively depending on the NetCentral system for critical device monitoring.

6. When you are satisfied with your settings, click the **Apply** button to put the settings into effect and leave the dialog box open, or click the **OK** button to save the settings and close the dialog box.
7. Click **Configure | Stop Heartbeat Polling**, then click **Configure | Start Heartbeat Polling**. If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts your changes into effect.

Managing NetCentral security

The following sections provide instructions for managing NetCentral security.

- [“Setting up NetCentral security levels and user groups” on page 113](#)
- [“Logging on to NetCentral manager” on page 114](#)
- [“Setting access rights to NetCentral manager features” on page 114](#)
- [“Access rights to NetCentral device-specific features” on page 116](#)
- [“Managing port access” on page 116](#)

Setting up NetCentral security levels and user groups

The NetCentral system has security levels based on Windows user groups. When you install NetCentral manager software on the NetCentral server, the install program creates three groups on the local PC for this purpose, as specified in the following table:

This security level...	Is based on this group...	With default access rights as follows:
Administrator	NCAdministrator	Can use and configure all NetCentral manager features. Can use and configure all device-specific features that are available through the NetCentral manager interface
Technician	NCTechnician	Can use all features to add/remove devices, monitor devices, and respond to status changes. Cannot customize the way the features operate, such as configuring actions or filtering messages.
User	NCUser	Can view status indicators, view settings, and browse subsystem status. Can not configure settings or in any way change the way information is displayed or processed.

The way in which you set up NetCentral system security depends in large part on the policies and conventions you use in your own system environment regarding user accounts, groups, and privileges.

From the NetCentral server, use standard procedures for your Windows operating system to assign groups to users. In Windows 2000 you can find the necessary settings at **Start | Settings | Control Panel | Users and Passwords | Advanced | Advanced**. All users are assigned to the NCUser group by default. NetCentral clients authenticate with the NetCentral server, so there is no need to assign groups to users at each NetCentral client.

Logging on to NetCentral manager

Whenever NetCentral is started, whether on the NetCentral server or on a NetCentral client, it starts up with user-level access permissions by default. Click **File | Logon** to log on to NetCentral with higher-level access permissions.

Setting access rights to NetCentral manager features

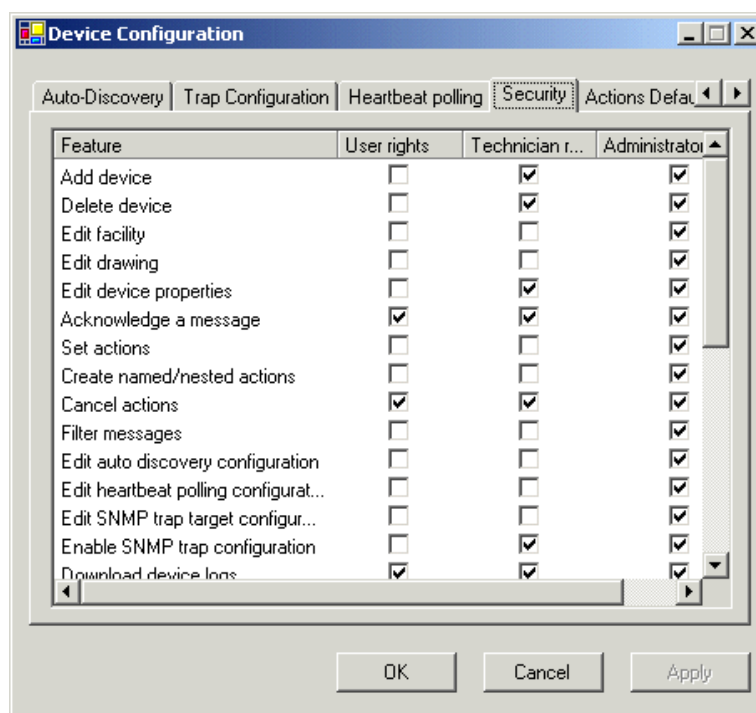
By default, NetCentral security levels have access to features as specified in the following table. The features listed here apply to all monitored device-types. Features not listed here have full access rights for all security levels:

Feature	User	Technician	Administrator
Add device	DENY	ALLOW	ALLOW
Delete device	DENY	ALLOW	ALLOW
Edit facility	DENY	DENY	ALLOW
Edit drawing	DENY	DENY	ALLOW
Edit device properties	DENY	ALLOW	ALLOW
Acknowledge a message	ALLOW	ALLOW	ALLOW
Set actions	DENY	DENY	ALLOW
Create named/nested actions	DENY	DENY	ALLOW
Cancel actions	ALLOW	ALLOW	ALLOW
Filter messages	DENY	DENY	ALLOW
Edit auto discovery configuration	DENY	DENY	ALLOW
Edit heartbeat polling configuration	DENY	DENY	ALLOW
Edit SNMP trap target configuration	DENY	DENY	ALLOW
Enable SNMP trap configuration (for device)	DENY	ALLOW	ALLOW
Download device logs	ALLOW	ALLOW	ALLOW
Edit Download device logs settings	DENY	DENY	ALLOW
Export NetCentral log	DENY	ALLOW	ALLOW
Edit NetCentral log views	DENY	ALLOW	ALLOW
Add remark	ALLOW	ALLOW	ALLOW
Clear messages	DENY	ALLOW	ALLOW
Run backup tool	DENY	DENY	ALLOW
Change Active drawing device image	DENY	DENY	ALLOW
Apply annotation	DENY	DENY	ALLOW
Add user defined tools	DENY	ALLOW	ALLOW
Launch configuration	DENY	DENY	ALLOW
Logout	DENY	DENY	ALLOW
Edit global action configuration	DENY	DENY	ALLOW

Feature	User	Technician	Administrator
Edit security configuration	DENY	DENY	ALLOW
Set SNMP trap target	DENY	DENY	ALLOW

You can modify security-level access to features as follows:

1. Make sure you are logged into NetCentral with administrator-level privileges.
2. Click **Configure | Security**. The System Settings dialog box opens. Click the **Security** tab.



3. For each level of security rights, select those features for which you are allowing access.
4. Click **OK** to save settings and close.

Access rights to NetCentral device-specific features

This section provides examples of the access rights that NetCentral manager grants to features that are specific to a certain device-type. In the same way that the features present on the menus vary depending on the currently selected device, so the access rights for features can vary depending on the currently selected device.

The following table includes features with consistent access rights between multiple device-types. Read your device-specific documentation regarding access rights for features that are unique to a single device type.

Device type	Device-type feature	Admin access rights	User access rights
All	Subsystem properties	View and edit	View only
All	Device configuration application	Launch of application allowed	Launch of application not allowed
Profile XP, Dell PowerEdge	Log download	View and edit settings Download logs	Download logs only
Cisco switch, Brocade switch	Port Alias	View and edit settings	View settings only

Managing port access

This section documents the ports the NetCentral system uses. If you intentionally restrict port access for security reasons, make sure that the NetCentral system has the necessary port access.

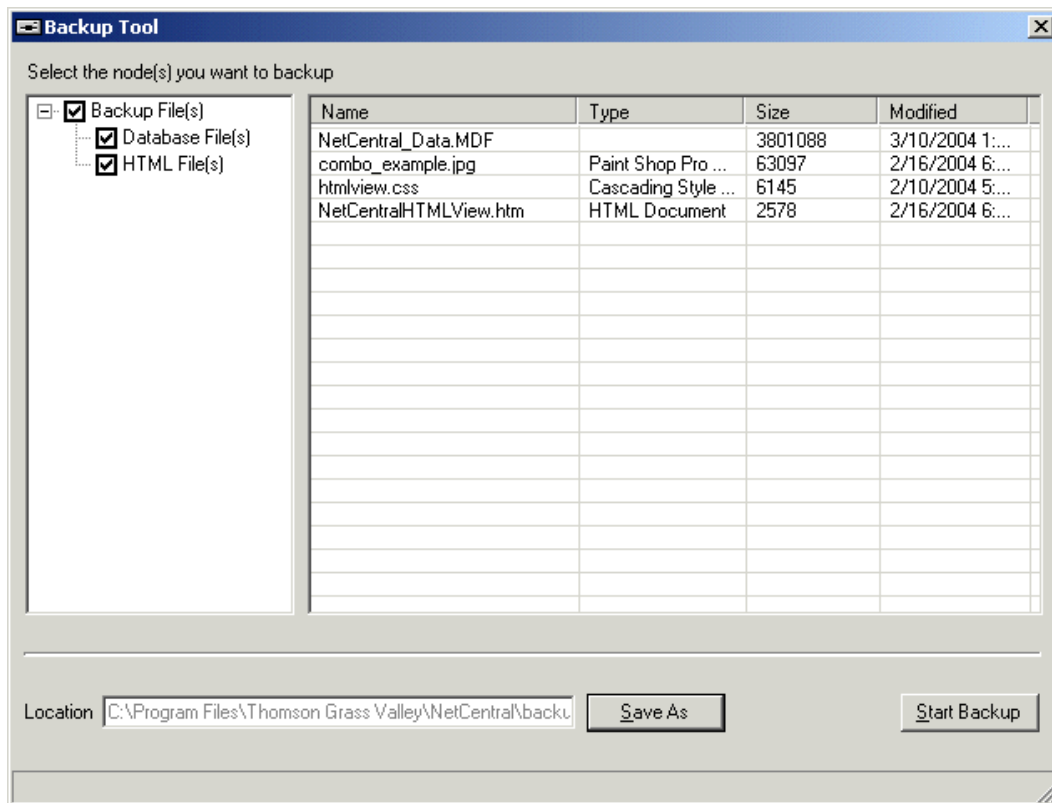
Feature/Function	NetCentral server port	Monitored device port	Other ports
Basic functions - These are the minimum ports required	162	161	—
Log access via FTP		21	—
Web-based configuration		80	—
Facility view files on remote host	—	—	80 - on the device hosting the web pages or files
Syslog monitoring	514	—	—
Mail actions	—	—	25 - on the SMTP server

Backing up the NetCentral database

You can create a backup copy of the NetCentral database and associated files. It is recommended that you do this periodically and store the backup copy on a network drive, on removable media, or in some other location from which it can be recovered in case of a system fault on the NetCentral server PC. All your configurations, such as devices added, actions, and messages, are stored in the NetCentral database, which resides on the NetCentral server PC only. NetCentral clients do not have their own copy of the database.

To back up the NetCentral database do the following:

1. On the NetCentral server PC, make sure there are no NetCentral automatic processes, such as Auto-discovery or SNMP trap configuration, currently executing. Check the Applications Log Viewer for indications of current processes.
2. Click **Tools | NetCentral Backup**. The Backup tool opens.



3. Select nodes in the tree view for the files and components to back up.
4. Click **Save As** and specify the backup location and file name.
5. Click **Start Backup**. Progress is reported in the bottom of the Backup Tool window. NetCentral saves the backup file as a ZIP file. A message box confirms when backup is complete.

To restore from the backup files, overwrite the files on the NetCentral server PC with the backup files from the .ZIP file.

Accommodating NetCentral database growth

Since the NetCentral database continues to capture and store messages as time goes on, it eventually become large enough that accommodation must be made for its continued growth. Logs downloaded from devices likewise need space.

To accommodate the growth of the NetCentral database and device-specific logs that you might download, make sure that you maintain at least 10 MB of free space on the NetCentral server disk that contains the NetCentral software and logs. This allows enough space to capture all your recent events, even during times of frequent activity.

To be sure that the NetCentral database does not grow beyond this space, the NetCentral manager software runs a daily check, at 3:07 am, on the size of the database. If the database size is approaching its size limit, NetCentral makes accommodation by running the following automatic processes:

- Roll up — With this process NetCentral gathers and saves statistics from the oldest messages in the database. These statistics are retained in the database and are available for research through the Graphs view.
- Purge — With this process NetCentral deletes the oldest messages from the database. This frees up space for new messages.

Setting up for remote access

If you want to monitor your devices from a location that is outside your facility's network, a NetCentral client can access the NetCentral server via Hypertext Transfer Protocol (HTTP) communication over the Internet. The .Net technology upon which NetCentral is built makes possible this type of remote access while retaining full features and functionality to the client.

While this access is possible, you will need to determine the steps to take according to your own security requirements, firewalls, and network infrastructure.

Verifying components installed and running

After installing NetCentral software and starting NetCentral manager on the server and on any clients, you can manually verify that the components necessary for the NetCentral system are running properly.

On the NetCentral server, check the Windows taskbar system tray for the following icons:

- NetCentral icon — When actively monitoring, the heartbeat graphic is moving and shows either a red or green color
- SQL icon — When services are running the icon shows a green triangle.

On the NetCentral server PC, click **Start | Settings | Control Panel | Administrative Tools | Services** and check the Windows Services Control panel for the following services:

Name	Status	Startup Type
MSSQLSERVER	Started	Automatic
MSSQLServerAdHelper		Manual
NetCentral 4.0 Action manager	Started	Manual
NetCentral 4.0 Active drawing	Started	Manual
NetCentral 4.0 Application logging	Started	Manual
NetCentral 4.0 Memory management	Started	Manual
NetCentral 4.0 Protocol Framework	Started	Manual
NetCentral 4.0 Security framework	Started	Manual
NetCentral 4.0 Syslog Service	Started	Automatic
NetCentralService	Started	Automatic
SNMP Trap Service		Manual
SQLSERVERAGENT		Manual

On a NetCentral client, check the Windows taskbar system tray for the following icons:

- NetCentral icon — When actively monitoring the heartbeat graphic is moving and shows either a red or green color

On a NetCentral client, check the Windows Services Control panel for the following services:

Name	Status	Startup Type
NetCentral 4.0 Action manager	Started	Manual
NetCentral 4.0 Active drawing	Started	Manual
NetCentral 4.0 Application logging	Started	Manual
NetCentral 4.0 Memory management	Started	Manual
NetCentral 4.0 Protocol Framework	Started	Manual
NetCentral 4.0 Security framework	Started	Manual
NetCentralService	Started	Automatic
SNMP Trap Service		Manual

Refer to [“Diagnosing NetCentral problems” on page 124](#) to test components.

Connecting a NetCentral client to a different NetCentral server

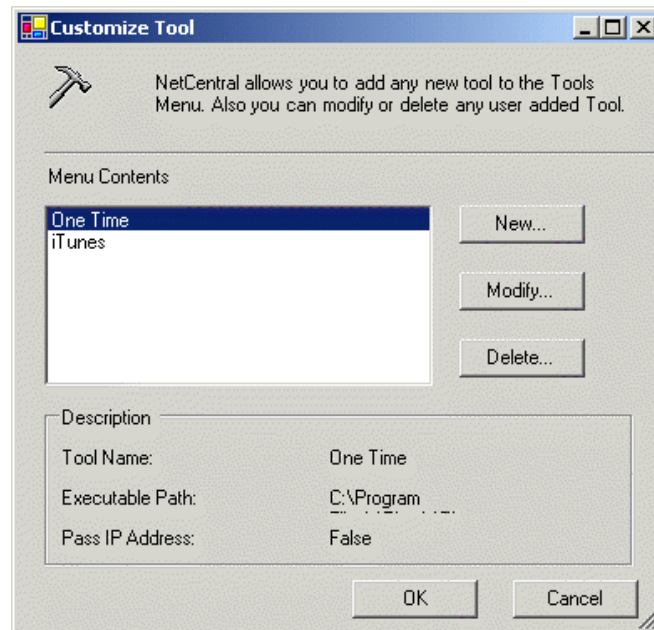
The NetCentral system does not support simultaneous or switching connections to multiple NetCentral servers from a single NetCentral client. If you must connect to a different server from a NetCentral client, do the following:

1. On the NetCentral client PC, uninstall the NetCentral client software. Use the standard procedures for your Windows operating system to uninstall software.
2. Reinstall the NetCentral client software as in [“Installing NetCentral software on clients” on page 32](#), and enter the IP address of the NetCentral server PC to which you now want to connect.
3. If the NetCentral server to which you are now connected has Graphical views set up or actions configured to files on the NetCentral server PC, you must copy the associated files to the NetCentral client such that their location is the same as that on the server.

Adding custom tools

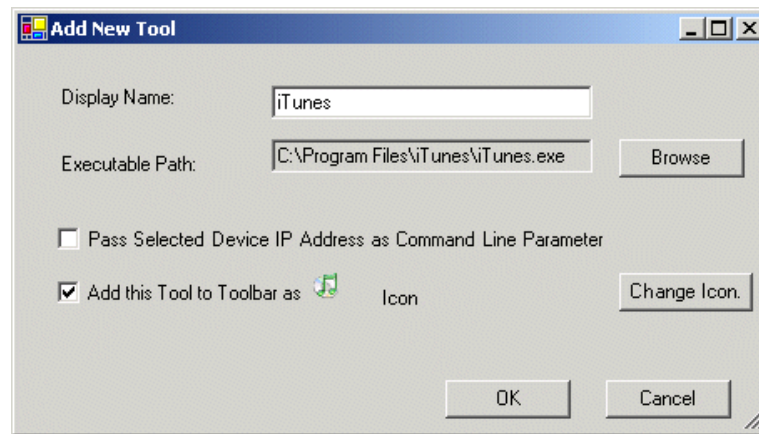
You can add your own program to the Tools menu as follows:

1. Log on to NetCentral with administrator-level privileges.
2. Click **Tools | Customize Tools**. The Customize Tools dialog box opens.



3. If custom tools have been added previously, click **Modify** or **Delete** to arrange the list of custom tools.

4. To add a new tool, click **New**. The Add New Tool dialog box appears.



5. Enter the name that you want displayed on the Tools menu.
6. Specify the location of the program file.
7. Specify if you want to pass the currently selected device's IP address to the tool.
8. Specify if you want the tool icon displayed. Select **Change Icon** to specify the icon.
9. Click **OK** on dialog boxes to save settings and close. Your custom tool appears on the Tools menu.
10. If you want your custom tools available from NetCentral client PCs, copy the program files to the same path on the client PCs.

Troubleshooting the NetCentral system

Use this section for problems with the NetCentral system itself. If the problem is actually on a monitored device and the NetCentral system is simply reporting the problem, troubleshoot the problem using the manual for the particular device.

Topics included in this section are as follows:

- [“Characterizing the problem” on page 123](#)
- [“Diagnosing NetCentral problems” on page 124](#)
- [“Restarting NetCentral services” on page 128](#)
- [“NetCentral troubleshooting guide” on page 129](#)

Characterizing the problem

Use the following questions to help you identify the characteristics of the problem. Characterizing the problem in this way will give you valuable clues about the cause of the problem and its solution.

- [“When does the problem occur?”](#)
- [“What is the behavior that indicates the problem?”](#)
- [“Where does the problem occur?”](#)
- [“What has changed?”](#)

When does the problem occur?

- Does the problem occur before or after certain other events?
- Does the problem occur as NetCentral opens?
- Does the problem occur after NetCentral is open and you try to accomplish a particular task?

What is the behavior that indicates the problem?

- Is an error message displayed?
- Does the entire application stop functioning, or do some parts still work?
- Is something displayed that you do *not* expect (such as an error message)?
- Is something *not* displayed that you *do* expect (such as a status indicator)?

Where does the problem occur?

- Are other similar functions working or are all similar functions having the same problem?
- Does the problem occur at the device level (viewing all devices at once) or at the subsystem level (viewing the details of one device only)?

- Is the problem associated with only some monitored devices or is the same for all monitored devices?
- Does the problem occur on one NetCentral client machine but not on other client machines?

What has changed?

- Since the last operation without the problem, have you changed anything within the NetCentral system?
- Since the last operation without the problem, have you changed anything within your Windows operating system?

Diagnosing NetCentral problems

You can evaluate the current operating status of your NetCentral system and diagnose problems using the tool described in this section. You can also diagnose problems using the troubleshooting guide later in this section.

About the NetCentral Diagnostic tool

The NetCentral Diagnostic tool is intended to be used primarily by Grass Valley Service personnel or by knowledgeable NetCentral users in cooperation with Grass Valley Service personnel. This tool is installed on the NetCentral server PC along with NetCentral manager software.

The NetCentral Diagnostic tool allows you to identify problems that can prevent your NetCentral system from fully functioning. These problems are usually the result of incorrect software setup. By running diagnostic tests on the various NetCentral software components, you can detect the following problems:

- Component not registered
- Component not present
- Component not licensed correctly
- Services or server components not installed

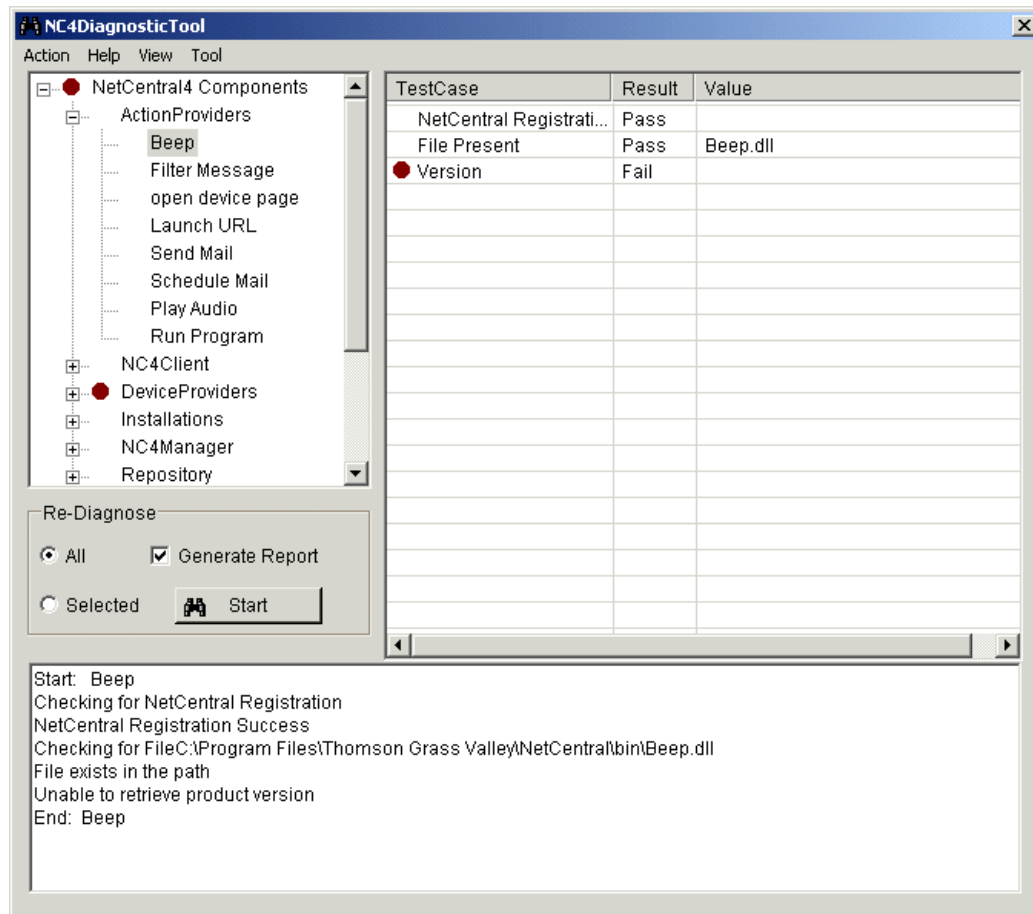
Running diagnostic tests on NetCentral components

Use the following procedure only after you have installed NetCentral manager software.

1. On the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges. If the NetCentral interface is inoperable, you can open the following file to start the Diagnostic Tool.

C:\Program Files\Thomson Grass Valley\NetCentral\bin\NC4DiagnosticToolClient.exe

2. Click **Tools | NetCentral Diagnostic**. The Diagnostic Tool application window opens.



3. Expand all nodes to see status indicators.
4. When the tool first runs, do the following:
 - a. Select **All** and **Generate Report**.
 - b. Click **Start**. The Save Report As dialog box opens.
 - c. Browse to the location to which you want to save the report file, rename the file if desired, and click **Save**.

The Diagnostic Tool tests your NetCentral system, displaying in the lower panel of the application window the test actions as they occur. These test actions are captured in the report file.
5. In the left panel of the application window, select a component about which you want to view diagnostic information. The results of the test on that component are displayed in the right panel of the application window.
6. To run a diagnostic test on a single component, do the following:
 - a. In the left panel of the application window, select the component you want to test.
 - b. Select **Selected**.

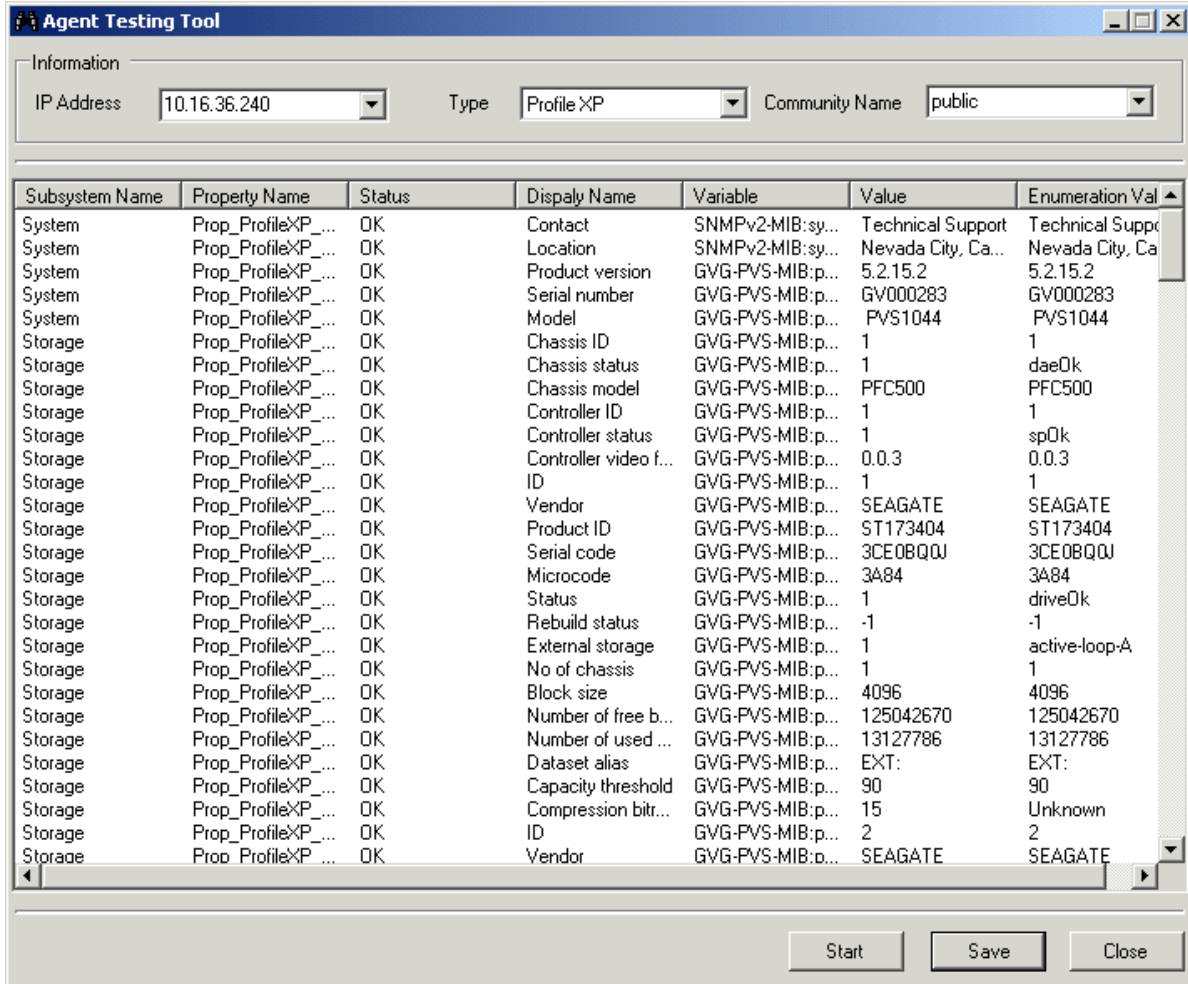
- c. Click **Start**. The Save Report As dialog box opens.
- d. Browse to the location to which you want to save the report file, rename the file if desired, and click **Save**.

The Diagnostic Tool tests the component, displaying in the lower panel of the application window the test actions as they occur. These test actions are captured in the report file.

Running diagnostic tests on a monitored device's SNMP agent

Use the following procedure only after you have installed NetCentral manager software.

1. On the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges.
2. Click **Tools | NetCentral Diagnostic**. The Diagnostic Tool application window opens. You can also open the Diagnostic tool from its file, as explained in [“Running diagnostic tests on NetCentral components” on page 124](#).
3. Click **Tool | Agent Testing Tool**. The Agent Testing Tool opens.



4. Specify the IP address, type, and SNMP community name of the monitored device.
5. Click **Start**. The tool runs the test and reports results in the window.
6. Click **Save** to save the report results as a text file.

Generating a list of all SNMP trap messages

You can generate a report that lists all of the SNMP trap messages that it is possible for a device-type to report through the NetCentral system.

To generate a list of all SNMP trap messages, do the following:

1. Click **Tools | Message Report**. The Message Report dialog box opens.
2. Select the device-type for which you want to view messages and generate the report. The report opens in a Web browser window. You can view or print the table from your browser.
3. Repeat for each device-type for which you want to view the list of SNMP trap messages.

About logs that contain NetCentral system information

This section refers to log information about the NetCentral system itself. For log-type information pertaining to the status of monitored devices, refer to [“Researching device status in NetCentral messages” on page 69](#) and [“Researching device-specific logs” on page 79](#).

A log is a historical record in text form of the events that occur on a system. As each event occurs, the logging mechanism inserts a new text entry into the log. By viewing this sequential progression of events, you can discover information that is valuable for maintaining and troubleshooting the system.

The NetCentral system captures its system information in several logs. These logs are displayed on tabs in the Application Logs window. The logs are as follows:

Discovery — Records the discovery process. Refer to [“Adding devices” on page 104](#).

Trap target — Records the SNMP trap configuration process. Refer to [“Setting automatic SNMP trap configuration” on page 109](#).

Keep Alive — Records the Heartbeat Polling process. Refer to [“Setting heartbeat polling” on page 111](#)

Actions — Records actions triggered. Refer to [“Configuring actions and notifications” on page 87](#).

Property — Records SNMP communication when property pages are manipulated. Refer to [“Browsing device status” on page 67](#).

Restarting NetCentral services

When you start the NetCentral interface on the NetCentral server PC, all the NetCentral services start. Refer to [“Verifying components installed and running” on page 118](#). If you then close the NetCentral interface on the NetCentral server PC, the NetCentral services continue to run. Refer to [“Stopping NetCentral” on page 48](#).

However, if the NetCentral software on the server PC becomes unresponsive, you can restart the NetCentral services, which allows the interface to function again.

To restart NetCentral services, do the following:

1. On the NetCentral server PC, open the **Stop NetCentral Services** shortcut on the Windows desktop or click **Start | Programs | NetCentral | Stop NetCentral Services**.

A Stop NetCentral Services command prompt window appears and shuts down services, which also closes the NetCentral interface. At the conclusion of its processes, the Stop NetCentral Services command prompt window restarts the NetCentral Service, then closes.

2. After the Stop NetCentral Services command prompt window closes, open the NetCentral interface. This restarts all the NetCentral services and restores functionality to the software.

NetCentral troubleshooting guide

The following table organizes problems according to when the problem occurs in relationship to the normal operating cycles of your operating system and applications. Scan the “When” and “What” columns to find information that correlates to the characteristics of your problem as determined in the previous section.

You can also use the NetCentral Application Logs to help troubleshoot problems. It is stored in the system’s temp directory and it is named *NCActivity.00*

When	What	Possible Cause	Corrective Action
At Windows startup	Error message: <i>The procedure entry point SnmpSvcGetEnterpriseO ID could not be located in the dynamic link library snmpapi.dll.</i>	When SNMP services was installed, system files were overwritten by incompatible versions.	Re-install the Windows Service Pack that is currently on your system to update all system files to compatible versions. Read Appendix D, Examples of Windows procedures .
	The NetCentral system does not start automatically when Windows starts	The NetCentral shortcut is not in the Windows Startup folder	Put a shortcut to NetCentral in the Windows startup folder.
	Unable to start the “Trap” engine in non-administrator log-ins	When NetCentral was installed and re-booted, the setup program was unable to register the software because the first log-in did not have administrator privileges. This is required because all NetCentral registrations are scheduled by the NetCentral setup program to the next reboot session.	Re-install NetCentral software and log-in with administrator privileges after first re-boot. Read “Managing NetCentral security” on page 113 .
At NetCentral startup	Error message: <i>Unable to start NetCentral. An error occurred while starting the SNMP trap engine. Make sure that you have the Microsoft SNMP Trap service correctly installed on the system.</i>	SNMP Trap Service is not installed or has been disabled.	Verify that SNMP Trap Service is installed and enabled.

When	What	Possible Cause	Corrective Action
	<p>Error message: <i>An error occurred while initializing the action provider playaudio.dll. NetCentral will be unable to trigger rules that are configured for this action provider.</i></p> <p>Error message: <i>NetCentral can not detect a sound card or a waveform audio device driver on this computer. This means that the "Play Audio" action will not be able to play audio files.</i></p>	Your PC does not have a sound card.	Install a sound card on your PC, or re-install the NetCentral software and answer "No" when prompted to install the play audio action provider.
	A new device on the local network is not automatically added to the NetCentral system.	Auto-Discovery settings have been changed from their defaults.	Check Auto-Discovery settings. Make sure "Never" is <i>not</i> selected and "Local" appears in the list. Read "Configuring Auto-discovery to add devices" on page 106.
	Unable to detect a device of a known type.	You are not licensed for monitoring that type of device.	Check whether you are running a licensed version of NetCentral. If you are running NetCentral Lite, it will detect the local Profile XP only. It will not detect any other Profile XP or any other device. You may view the Application Logs to check for any licensing violations.
		Device is not accessible	Ensure that the device is on the network and can be accessed from the NetCentral server.
		SNMP agent is not working correctly on the device	Ensure that the SNMP agent is running on the device and check whether it is correctly configured. Some agents allow you to accept SNMP packets only from specific computers. Make sure that the SNMP agent will accept SNMP packets from the NetCentral server.
		SNMP community names on device and NetCentral server do not match.	Ensure that the SNMP community name, such as "public", used by NetCentral during discovery matches the one set on the device. Read "Setting automatic SNMP trap configuration" on page 109.
		Device provider is not registered.	Ensure that the provider for that device is registered. To check whether a device provider is registered, use the Diagnostic tool as explained in "Running diagnostic tests on NetCentral components" on page 124.
	Cannot open databases or a database error is reported via a message box or via the Application logs.	Hard drive is full	Check whether there is sufficient disk space on the hard-drive where the NetCentral software is installed. Read "Accommodating NetCentral database growth" on page 118.

When	What	Possible Cause	Corrective Action
			Send all the Application logs generated by NetCentral to technical support for detailed analysis.
You try to view a device-specific log that is listed on the menu	You are unable to view the log	FTP service on the device is not running correctly	Check whether the FTP service is running on the device and is correctly installed on the device as per the device's documentation.
		Logs directory on Profile XP is not accessible.	Using a Web-browser, go to URL: <i>ftp://<profilename or IP address>/log</i> . If this does not list the logs directory on the Profile, troubleshoot your network to re-establish access.
A reportable event occurs on a monitored device.	The event is not reported by fault messages or status indicators on the NetCentral server.	Messages (SNMP traps) sent from the device do not have the IP address of the NetCentral server embedded.	Configure SNMP properties on the device. Read "Set SNMP trap destinations on monitored devices" on page 39.
		SNMP Trap Service is not running on the NetCentral server or client.	Go to Control Panel Services and start the SNMP Trap Service.
	The "Play Audio" action should play a sound, but no sound is heard.	Sound card not installed or has been disabled on PC.	Verify that a sound card is installed and enabled by checking Control Panels Multimedia and Control Panels Devices. Install or enable accordingly
		Speakers not plugged in or not powered up.	Plug in speakers and verify proper power supply.
		The audio file to be played is not a "WAV" format file.	Reconfigure the action to play a Wave file. Read "Playing a sound file" on page 94.
			To test your system, locate some "WAV" files in the WINNT\System32\Media Files directory on your computer and double-click the file. If the computer is unable to play the file, there is an error with the multi-media software installed on your computer.
	An e-mail should be sent, but it doesn't go through.	SMTP configuration wrong or the SMTP server is down.	Re-configure properties for e-mail actions and test. Check whether the SMTP server name or IP address specified is correct. Check whether the "from" e-mail address is valid and has a valid log-in on the SMTP server. Read "Sending e-mail and pager notifications" on page 91.
	Two identical SNMP trap messages appear.	The device has two SNMP trap destinations for the NetCentral server: one as a name and one as an IP address	Reconfigure trap destinations on the monitored device and make sure each NetCentral server is entered but once.

Graphical view tutorial

This tutorial provides procedures for creating active drawings and their indicators, such as would typically be combined in a large-scale diagram. Work through the tutorial to understand the advanced features, then apply them as appropriate to create the Graphical views required for your own system environment.

Topic included in this tutorial are as follows:

- [“Preparations” on page 133](#)
- [“Propagating the Graphical view to NetCentral client PCs” on page 134](#)
- [“Creating a custom view of monitored devices” on page 135](#)
- [“Executing a program” on page 140](#)
- [“Applying an annotation layer” on page 142](#)
- [“Placing a folder icon onto the HTML page” on page 142](#)

Preparations

Before you actually begin creating a graphical view, you should make the following preparations:

- [“Prerequisite skills and system requirements” on page 133](#)
- [“Requirements” on page 134](#)
- [“Design” on page 134](#)
- [“Resources” on page 134](#)

Prerequisite skills and system requirements

To best understand and apply this tutorial, make sure you are familiar with HTML coding and Web site development, including the following basic skills:

- Creating Web pages
- Creating images
- Referencing images in Web Pages
- Hyperlinking Web Pages

The default NetCentral HTML editing tool is used in the procedures in this tutorial. However, you might want to use a different HTML editing tool that supports .NET objects, such as a recent version of Microsoft Front Page. If you use a different HTML editing tool, you must apply your knowledge of the tool and of standard Web development techniques to determine how to integrate the tool with NetCentral Graphical view features.

Requirements

You should define the requirements for your monitoring needs. The following questions can help you define your requirements:

- What status information is most important to see at a glance?
- How do you want your devices organized? By physical location? By logical system? By signal path? By device-type? If by multiple organizational schemes, how do you want the schemes layered and interlinked?
- How much screen space will you use for your day-to-day monitoring view? A Taskbar icon only with no NetCentral window open? A single NetCentral window open? Multiple NetCentral windows open on a single monitor? Multiple NetCentral windows open on multiple monitors?

Design

From your requirements, design one or more graphical view pages. Then design a Tree view hierarchical structure that provides a folder to which each of your graphical view pages can be linked.

Resources

To create the pages demonstrated in this tutorial, the following resources are used. For many of these resources, you can use those supplied by default with the NetCentral system, or you can create your own customized versions. When these resources are procured, place them in the locations indicated so as to be available as you create the Graphical view pages.

- Background images — Default files are located at:

C:\Program Files\Thomson Grass Valley\NetCentral\HTML

- Device Images — Default files for gray, yellow, and red images to indicate status levels are located at:

C:\Program Files\Thomson Grass Valley\NetCentral\bin\imagelibrary\<devicetype>

- Programs — Default programs are located at:

C:\Program Files\Thomson Grass Valley\NetCentral\bin

Propagating the Graphical view to NetCentral client PCs

If you have NetCentral client PCs, you must adopt a mechanism for propagating your graphical views to them. This is necessary because NetCentral accesses the HTML files and images identically from NetCentral client PCs and from the NetCentral server PC. Some of the mechanisms that allow this access are as follows:

- Copy files onto all client PCs — Set up all your files using a specified path on the local drive of the NetCentral server PC. When you are done with your graphical views, copy the files to the same specified path location on all client PCs.
- Put files on a shared network drive — Set up all your files on a network drive that is accessible from the server PC and all client PCs. Map the drive on the server PC

and on all client PCs so that its path is identical.

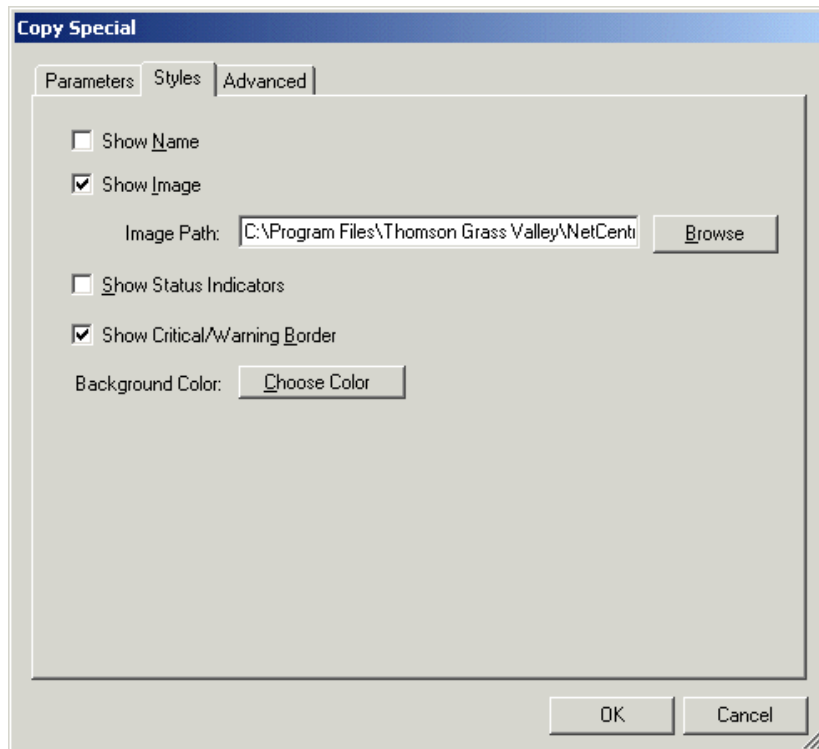
- Serve files from a Web server — Post files on a Web server that is accessible from server PC and client PCs and use http links as you develop your graphical views.

Chose the mechanism that is appropriate for your facility and adapt your graphical view development techniques accordingly.

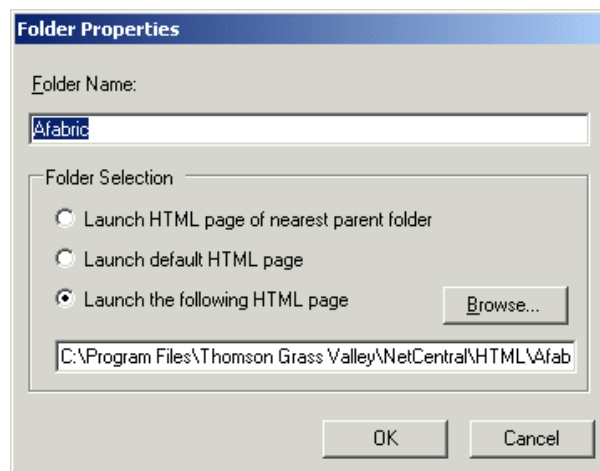
Creating a custom view of monitored devices

This procedure allows you to use your own HTML files, background images, dynamic indicators, and other HTML development techniques rather than those provided by default through the “Create HTML View” feature.

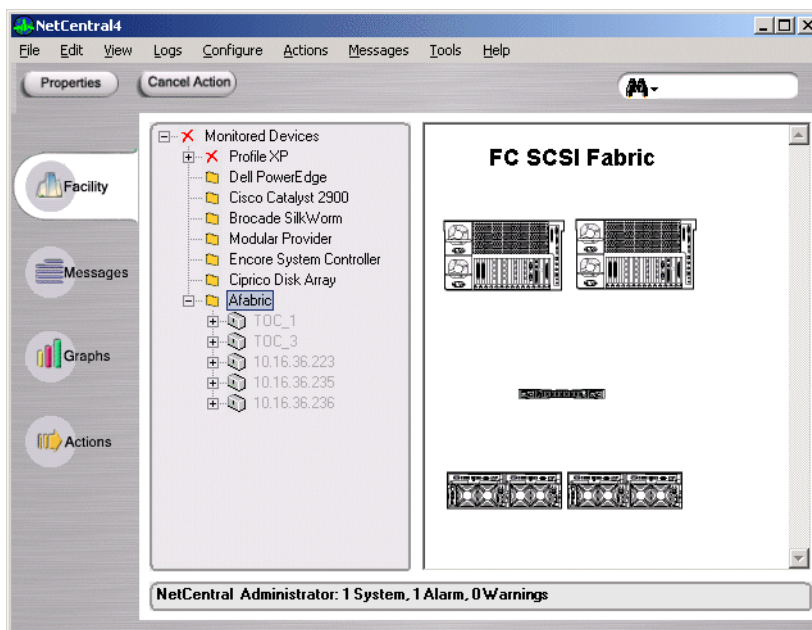
1. From the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges.
2. Create and save a HTML page that you intend to associate with one of the folders in the Tree View. Add a background image to the page if required. Refer to [“Creating a Facility graphical view” on page 57](#) for the default procedure.
3. In NetCentral, click **File | HTML Page | Open** and open the HTML page in the NetCentral HTML editor.
4. In the NetCentral Tree view, right-click a device that you intend to place on the HTML page and select **Copy Special**. The Copy Special dialog box opens. Click the **Styles** tab.



5. Specify the image file for the device.
6. Select the type of status indicator for the device image as follows:
 - Show status indicators — This puts a LED-type colored indicator adjacent to the image.
 - Show critical/warning border — This surrounds the image with a colored border for critical and warning status conditions.
7. Click **OK**. The active drawing with image as you have specified is now on the clipboard.
8. In the HTML editor, paste the active drawing onto the HTML page.
9. Repeat the previous steps to place more active drawings on the page.
10. Arrange active drawings on the page.
11. Add text or otherwise format as required.
12. Save the HTML file.
13. In the Facility view, right-click a folder and select **Properties**. The Folder Properties dialog box opens.



14. Select **Launch the following HTML page**, specify your HTML page, and click **OK**.
15. In NetCentral, right-click the Facility view information area or click **View** and select **Refresh**.
16. Select the folder and your custom graphical view appears.



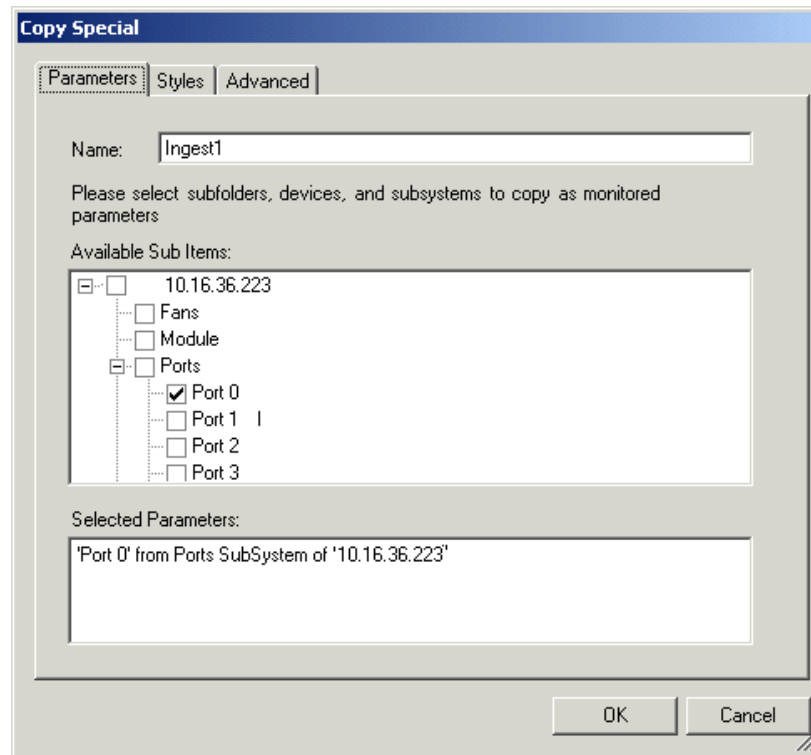
Adding subsystem indicators

Subsystem indicators are colored blocks that can be sized and placed around a device to represent a subsystem of that device. The connector can show the current status of the subsystem or parameter it represents.

To add subsystem connectors do the following:

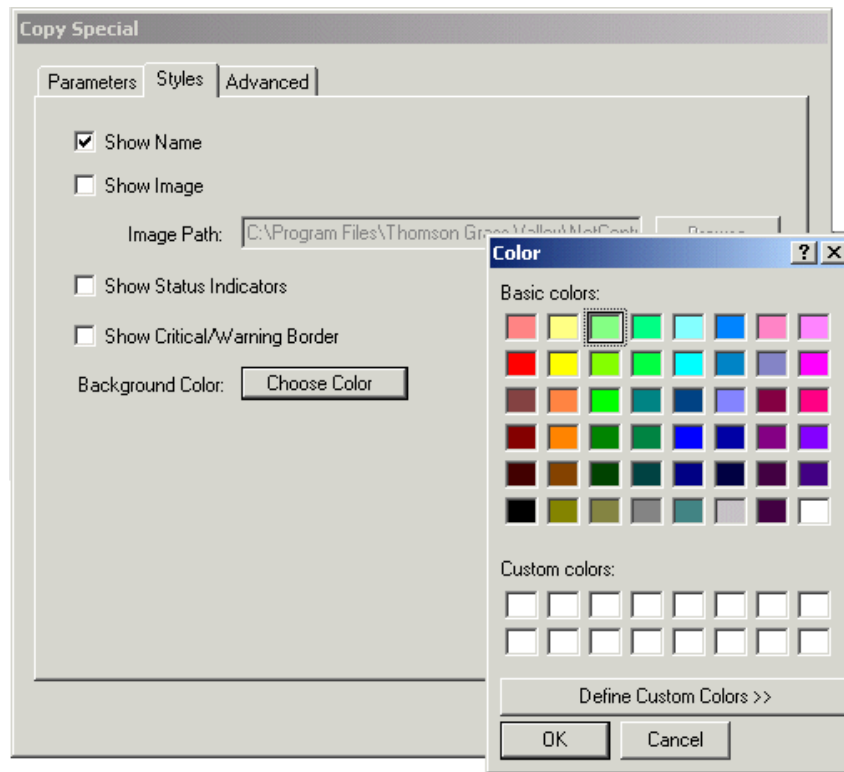
1. From the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges.
2. Open one of your graphical view HTML pages in the NetCentral HTML editor. If the page is associated with a Tree view folder, right-click the folder and select **HTML Page**. The page opens in the NetCentral HTML editor.

3. In the NetCentral Tree view, right-click a device in the folder, such as a Fibre Channel switch, and select **Copy Special**. The Copy Special dialog box opens. Click the **Parameters** tab.



4. Deselect the device node at the top of the tree, then select one or more subsystems or parameters. For example, for a Fibre Channel switch you can select the parameter for an individual port. This allows you to create an indicator for that port, so you can monitor the connectivity of the data flow it carries.
5. Name the subsystem or parameter that you have selected.

6. Click the **Styles** tab.



7. Select **Show Name**.

8. Deselect other checkboxes.

9. Click **Choose Color**. The Color dialog box opens.

10. Select the color to represent your selected parameter.

11. Click **OK** on dialog boxes to save settings and close.

12. In the HTML editor, paste the indicator for the parameter. It appears as a colored block.

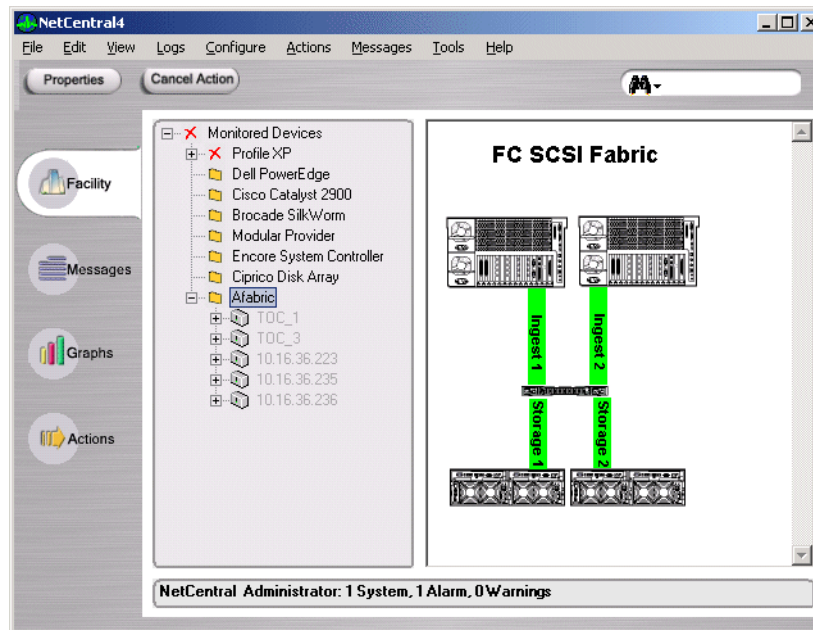
13. Resize and arrange the indicator to represent the parameter.

14. Repeat the previous steps to place more subsystem or parameter indicators on the page.

15. Save the HTML file.

16. In NetCentral, right-click the Facility view information area or click **View** and select **Refresh**.

17. Select the folder and your HTML page appears. The indicators change color when a status change occurs.



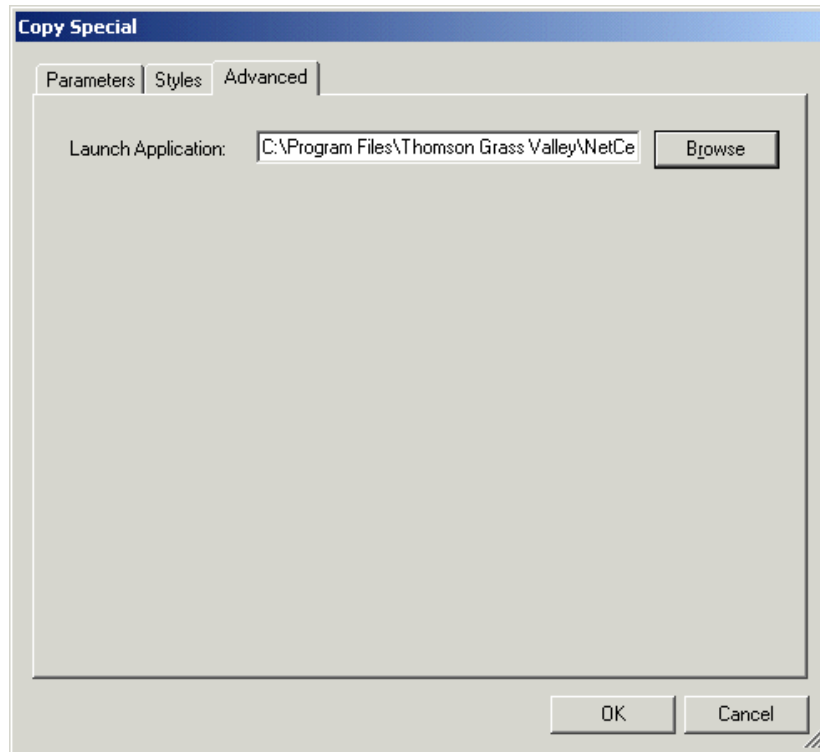
Executing a program

You can configure NetCentral so that when you click a device on a HTML page, NetCentral launches a program of your choice.

To set the program you want to launch do the following:

1. From the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges.
2. In NetCentral, click **File | HTML Page | Open** and open the HTML page from which you want to launch the program.

3. In the NetCentral Tree view, right-click a device and select **Copy Special**. The Copy Special dialog box opens. Click the **Advanced** tab.



4. Specify the program file that you want launched.
5. Click **OK**.
6. In the HTML editor, paste in the active drawing.
7. Save the HTML page.
8. In NetCentral, right-click the Facility view information area and select **Refresh**.
9. Select the folder for the HTML page and click the active drawing. The program launches.
10. If you want to launch the program from NetCentral client PCs, copy the program file to the same path on the client PCs.

Applying an annotation layer

All of the active objects that you place on an HTML page — such as devices, subsystems, and folders — together comprise an annotation layer that is independent of the background of the HTML page. You can copy an annotation layer intact from one HTML page and apply it to another HTML page. In this way you can create modified versions of the same view of equipment without re-building the annotation layer from the beginning for each version.

This feature is especially useful if you are basing several HTML pages on a standard background image.

To apply an annotation layer, do the following:

1. From the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges.
2. Click **File | HTML Page | Open** and open the HTML page to which you want to add an annotation layer.
3. In the HTML Editor, click **Edit | Apply Annotations**. The OverlayImageApplier dialog box opens. Browse to the file or enter the path and name of the file that contains the annotation layer that you want to copy. Click **OK** to close dialog boxes and **OK** on the "...successful..." message. The active components that make up the annotation layer appear on the HTML page.
4. On the HTML Editor, click **File | Save**.

Placing a folder icon onto the HTML page

In the same way that you can place a device on a HTML page, you can also place a folder on a HTML page. When you do this the folder is represented by an icon on the page. If the folder itself is associated with a HTML page, its icon becomes a hyperlink to the HTML page.

To place a folder icon onto a HTML page, do the following:

1. From the NetCentral server PC, make sure you are logged into NetCentral with administrator-level privileges.
2. Click **File | HTML Page | Open** and open the HTML page to which you want to add a folder. The HTML Editor opens.
3. In the Tree view, right-click the folder whose icon you want to place on the HTML page and select **Copy**.
4. In the HTML Editor paste the folder active drawing onto the page.
5. Save the HTML page.
6. In NetCentral, right-click the Facility view information area or click **View** and select **Refresh**.
7. Select the folder for the HTML page and click the folder active drawing. The HTML page for the folder active drawing opens.

Simple Network Management Protocol tutorial

This tutorial explains Simple Network Management Protocol (SNMP)

Topic included in this tutorial are as follows:

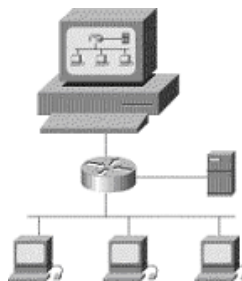
- [“Introduction to SNMP” on page 143](#)
- [“SNMP Version 1” on page 146](#)
- [“SNMP Version 2” on page 149](#)
- [“SNMP Version 3” on page 153](#)
- [“NetCentral as Trilingual Network-Management System” on page 156](#)
- [“What Libraries to Use?” on page 158](#)
- [“References” on page 159](#)

Introduction to SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Three versions of SNMP exist: SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) and SNMP version 3 (SNMPv3). All versions have a number of features in common, but SNMPv2 and SNMPv3 offer enhancements, such as additional protocol operations and security aspects.

SNMP Facilitates the Exchange of Network Information Between Devices



SNMP Basic Components

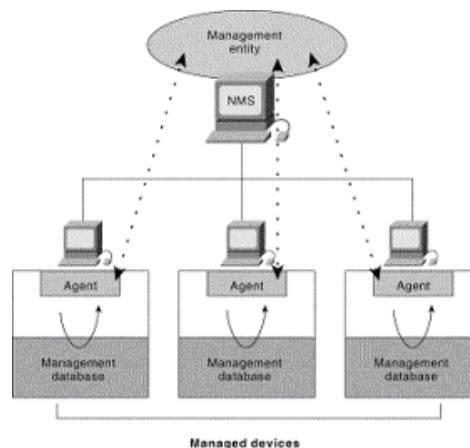
An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

The following figure illustrates the relationships of these three components.



SNMP Basic Commands

Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations.

The read command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

The write command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.

The trap command is used by managed devices, to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.

Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

SNMP Management Information Base

A Management Information Base (MIB) is a collection of information that is organized hierarchically. MIBs are accessed using a network-management protocol such as SNMP. They are comprised of managed objects and are identified by object identifiers

A managed object (sometimes called a MIB object, an object, or a MIB) is one of any number of specific characteristics of a managed device. Managed objects are comprised of one or more object instances, which are essentially variables.

Two types of managed objects exist: scalar and tabular. Scalar objects define a single object instance. Tabular objects define multiple related object instances that are grouped in MIB tables

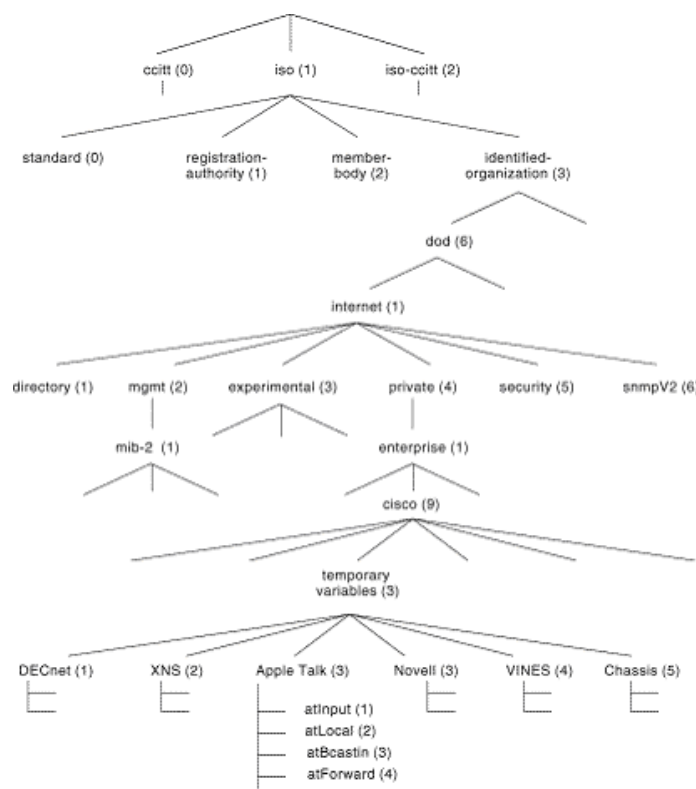
An example of a managed object is `atInput` (See next figure), which is a scalar object that contains a single object instance, the integer value that indicates the total number of input AppleTalk packets on a router interface

An object identifier (or object ID) uniquely identifies a managed object in the MIB hierarchy. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. Figure 2 illustrates the MIB tree

The top-level MIB object IDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations

Vendors can define private branches that include managed objects for their own products. MIBs that have not been standardized typically are positioned in the experimental branch

The managed object `atInput` can be uniquely identified either by the object name — `iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.variables.AppleTalk.atInput` — or by the equivalent object descriptor, `1.3.6.1.4.1.9.3.3.1`.



SNMP and Data Representation

SNMP must account for and adjust to incompatibilities between managed devices. Different computers use different data representation techniques, which can compromise the capability of SNMP to exchange information between managed devices. SNMP uses a subset of Abstract Syntax Notation One (ASN.1) to accommodate communication between diverse systems.

SNMP Version 1

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. It is described in Request For Comments (RFC) 1157 and functions within the specifications of the Structure of Management Information (SMI). SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX).

SNMPv1 and Structure of Management Information

The Structure of Management Information (SMI) defines the rules for describing management information, using Abstract Syntax Notation One (ASN.1). The SNMPv1 SMI is defined in RFC 1155. The SMI makes three key specifications: ASN.1 data types, SMI-specific data types, and SNMP MIB tables.

SNMPv1 and ASN.1 Data Types

The SNMPv1 SMI specifies that all managed objects have a certain subset of Abstract Syntax Notation One (ASN.1) data types associated with them. Three ASN.1 data types are required: name, syntax, and encoding. The name serves as the object identifier (object ID). The syntax defines the data type of the object (for example, integer or string). The SMI uses a subset of the ASN.1 syntax definitions. The encoding data describes how information associated with a managed object is formatted as a series of data items for transmission over the network.

SNMPv1 and SMI-Specific Data Types

The SNMPv1 SMI specifies the use of a number of SMI-specific data types, which are divided into two categories: simple data types and application-wide data types

Three simple data types are defined in the SNMPv1 SMI, all of which are unique values: integers, octet strings, and object IDs. The integer data type is a signed integer in the range of -2,147,483,648 to 2,147,483,647. Octet strings are ordered sequences of 0 to 65,535 octets. Object IDs come from the set of all object identifiers allocated according to the rules specified in ASN.1

Seven application-wide data types exist in the SNMPv1 SMI: network addresses, counters, gauges, time ticks, opaques, integers, and unsigned integers.

Network addresses represent an address from a particular protocol family. SNMPv1 supports only 32-bit IP addresses.

Counters are non-negative integers that increase until they reach a maximum value and then return to zero. In SNMPv1, a 32-bit counter size is specified.

Gauges are non-negative integers that can increase or decrease but that retain the maximum value reached.

A time tick represents a hundredth of a second since some event.

An opaque represents an arbitrary encoding that is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.

An integer represents signed integer-valued information. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

An unsigned integer represents unsigned integer-valued information and is useful when values are always non-negative. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

SNMP MIB Tables

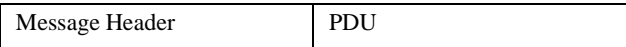
The SNMPv1 SMI defines highly structured tables that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables are composed of zero or more rows, which are indexed in a way that allows SNMP to retrieve or alter an entire row with a single Get, GetNext, or Set command.

SNMPv1 Protocol Operations

SNMP is a simple request/response protocol. The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: Get, GetNext, Set, and Trap. The Get operation is used by the NMS to retrieve the value of one or more object instances from an agent. If the agent responding to the Get operation cannot provide values for all the object instances in a list, it does not provide any values. The GetNext operation is used by the NMS to retrieve the value of the next object instance in a table or a list within an agent. The Set operation is used by the NMS to set the values of object instances within an agent. The Trap operation is used by agents to asynchronously inform the NMS of a significant event.

SNMPv1 Message Formats

SNMPv1 messages contain two parts: a message header and a protocol data unit (PDU). Figure 4 illustrates the basic format of an SNMPv1 message.



SNMPv1 Message Header

SNMPv1 message headers contain two fields: Version Number and Community Name.

The following descriptions summarize these fields:

- Version number — Specifies the version of SNMP used.
- Community name — Defines an access environment for a group of NMSs. NMSs within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

SNMPv1 Protocol Data Unit

SNMPv1 PDUs contain a specific command (Get, Set, and so on) and operands that indicate the object instances involved in the transaction. SNMPv1 PDU fields are variable in length, as prescribed by ASN.1. The following table illustrates the fields of the SNMPv1 Get, GetNext, Response, and Set PDUs transactions.

PDU type	Request ID	Error status	Error index	Object 1 value 1	Object 2 value 2	Object x value x
Variable bindings						

The following descriptions summarize the fields:

- PDU type — Specifies the type of PDU transmitted.
- Request ID — Associates SNMP requests with responses.
- Error status — Indicates one of a number of errors and error types. Only the response operation sets this field. Other operations set this field to zero.

- Error index — Associates an error with a particular object instance. Only the response operation sets this field. Other operations set this field to zero.
- Variable bindings — Serves as the data field of the SNMPv1 PDU. Each variable binding associates a particular object instance with its current value (with the exception of Get and GetNext requests, for which the value is ignored).

Trap PDU Format

Figure 6 illustrates the eight fields of the SNMPv1 Trap PDU.

Enterprise	Agent address	Generic trap type	Specific trap code	Time Stamp	Object 1 value 1	Object 2 value 2	Object x value x
Variable bindings							

The following descriptions summarize the fields illustrated in Figure 6:

- Enterprise — Identifies the type of managed object generating the trap.
- Agent address — Provides the address of the managed object generating the trap.
- Generic trap type — Indicates one of a number of generic trap types.
- Specific trap code — Indicates one of a number of specific trap codes.
- Time stamp — Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.
- Variable bindings — The data field of the SNMPv1 Trap PDU. Each variable binding associates a particular object instance with its current value

SNMP Version 2

SNMP version 2 (SNMPv2) is an evolution of the initial version, SNMPv1. Originally, SNMPv2 was published as a set of proposed Internet standards in 1993; currently, it is a draft standard. As with SNMPv1, SNMPv2 functions within the specifications of the Structure of Management Information (SMI). In theory, SNMPv2 offers a number of improvements to SNMPv1, including additional protocol operations.

SNMPv2 and Structure of Management Information

The Structure of Management Information (SMI) defines the rules for describing management information, using ASN.1

The SNMPv2 SMI is described in RFC 1902. It makes certain additions and enhancements to the SNMPv1 SMI-specific data types, such as including bit strings, network addresses, and counters. Bit strings are defined only in SNMPv2 and comprise zero or more named bits that specify a value.

Network addresses represent an address from a particular protocol family. SNMPv1 supports only 32-bit IP addresses, but SNMPv2 can support other types of addresses as well.

Counters are non-negative integers that increase until they reach a maximum value and then return to zero.

In SNMPv1, a 32-bit counter size is specified. In SNMPv2, 32-bit and 64-bit counters are defined.

SMI Information Modules

The SNMPv2 SMI also specifies information modules, which specify a group of related definitions. Three types of SMI information modules exist: MIB modules, compliance statements, and capability statements. MIB modules contain definitions of interrelated managed objects. Compliance statements provide a systematic way to describe a group of managed objects that must be implemented for conformance to a standard. Capability statements are used to indicate the precise level of support that an agent claims with respect to a MIB group. An NMS can adjust its behavior toward agents according to the capabilities statements associated with each agent.

SNMPv2 Protocol Operations

The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2. However, SNMPv2 adds and enhances some protocol operations. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and is designed to replace the SNMPv1 Trap

SNMPv2 also defines two new protocol operations: GetBulk and Inform.

The GetBulk operation is used by the NMS to efficiently retrieve large blocks of data, such as multiple rows in a table. GetBulk fills a response message with as much of the requested data as will fit. The Inform operation allows one NMS to send trap information to another NMS and to then receive a response. In SNMPv2, if the agent responding to GetBulk operations cannot provide values for all the variables in a list, it provides partial results

The InformRequest PDU is sent by an SNMPv2 entity acting in a manager role, on behalf of an application, to another SNMPv2 entity acting in a manager role, to provide management information to an application using the latter entity. When an InformRequest PDU is received, the receiving SNMPv2 sends a response PDU with the same values in its *request-id* and *variable-bindings* fields.

SNMPv2 Message Format

SNMPv2 messages consist of a header and a PDU. Figure 7 illustrates the basic format of an SNMPv2 message.



SNMPv2 Message Header

SNMPv2 message headers contain two fields: Version Number and Community Name.

The following descriptions summarize these fields:

- Version number — Specifies the version of SNMP that is being used.

- Community name — Defines an access environment for a group of NMSs. NMSs within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

SNMPv2 Protocol Data Unit

SNMPv2 specifies two PDU formats, depending on the SNMP protocol operation. SNMPv2 PDU fields are variable in length, as prescribed by Abstract Syntax Notation One (ASN.1)

Figure 8 illustrates the fields of the SNMPv2 Get, GetNext, Inform, Response, Set, and Trap PDUs

The following descriptions summarize the fields illustrated in Figure 8:

- PDU type — Identifies the type of PDU transmitted (Get, GetNext, Inform, Response, Set, or Trap).
- Request ID — Associates SNMP requests with responses.
- Error status — Indicates one of a number of errors and error types. Only the response operation sets this field. Other operations set this field to zero.
- Error index — Associates an error with a particular object instance. Only the response operation sets this field. Other operations set this field to zero.
- Variable bindings — Serves as the data field of the SNMPv2 PDU. Each variable binding associates a particular object instance with its current value (with the exception of Get and GetNext requests, for which the value is ignored).

PDU type	Request ID	Error status	Error index	Object 1 value 1	Object 2 value 2	Object x value x
Variable bindings						

GetBulk PDU Format

Figure 9 illustrates the fields of the SNMPv2 GetBulk PDU.

PDU type	Request ID	Non-repeaters	Max repetitions	Object 1 value 1	Object 2 value 2
Variable bindings					

One of the major enhancements SNMPv2 provides the GetBulkRequest PDU. Its purpose is to minimize the number of protocol exchanges required to retrieve large amount management information.

The GetBulkRequest works in the following way. The GetBulkRequest includes a list of (N + R) variable names in the variable-bindings list. For each of the first N names, retrieval takes place as for GetNextRequest. This is, for each variable in the list, the

next variable in lexicographic order plus its value are returned; if there is no lexicographic successor, then the named variable and a value of *endOfMibView* are returned.

The GetBulkRequest PDU has two fields not found in the other PDUs: non-repeaters and max-repetitions. The field specifies the number of variables in the variable-bindings list for which a single lexicographic successor is to be returned. The max-repetitions field specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list.

Example:

If an SNMP Manager issues request with six variable names; for the first two variables (non-repeaters = 2), a single values is requested; for the remaining variables, six successive values (max-repetitions = 6) are requested.

Manager: GetBulkRequest (non-repeaters = 2, max-repetitions = 6, X, Y, TA, TB, TC)

Agent: Response [X, Y, TA (1), TB (1), TC (1),
TA (2), TB (2), TC (2),
TA (3), TB (3), TC (3),
TA (4), TB (4), TC (4),
TA (5), TB (5), TC (5),
TA (6), TB (6), TC (6)].

The following descriptions summarize the fields illustrated in Figure -9:

- PDU type — Identifies the PDU as a GetBulk operation.
- Request ID — Associates SNMP requests with responses.
- Non-repeaters — Specifies the number of object instances in the variable bindings field that should be retrieved no more than once from the beginning of the request. This field is used when some of the instances are scalar objects with only one variable.
- Max repetitions — Defines the maximum number of times that other variables beyond those specified by the Non-repeaters field should be retrieved.
- Variable bindings — Serves as the data field of the SNMPv2 PDU. Each variable binding associates a particular object instance with its current value (with the exception of Get and GetNext requests, for which the value is ignored).

SNMPv2 Trap PDU Format

The SNMPv2-Trap PDU is generated and transmitted by SNMPv2 entity acting in an agent role when an unusual event occurs. This PDU fulfills the same role as the SNMPv1-Trap PDU, but with a different format. The SNMPv2-Trap PDU uses the same format as all other SNMPv2 PDUs except GetBulkRequest, thus easing the processing task at the receiver

The variable-bindings field in the SNMPv2-Trap PDU contains the following pairs of object names and values:

- sysUpTime.0
- snmpTrapOID.0: part of the trap group in the SNMPv2 MIB.
- Additional variables may be included at the option of the agent

As with the SNMP Trap PDU, no response is issued to an SNMPv2-Trap PDU

SNMP Version 3

The version 3 of Simple Network Management Protocol addresses some of the long pending issues related to the large-scale deployment of SNMP for configuration, accounting and fault management.

Currently SNMP is predominantly used for monitoring and performance management. Due to lack of security with the use of SNMP, system and network administrators were using other means like telnet, ASCII etc. for configuration, accounting and fault management. The primary goal of SNMP version 3 (SNMPv3) is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities, which make remote administration of SNMP entities a much simpler task.

- The SNMPv1 and v2c protocols, which have a wide deployment base covers the following
- A platform independent data definition syntax - A subset of Abstract Syntax Notation1 (ASN.1).
- A platform independent data transfer notation - Basic Encoding Rule (BER)
Communication between the peer entities - SNMP communication protocol with message formats, message types etc.
 - Message contains the SNMP protocol version
 - Message contains the community string which is used to provide some security
- Guidelines for definition of management data - The Structure of Management Information
- Management data definition repository - various MIB files.

What SNMPv3 Covers?

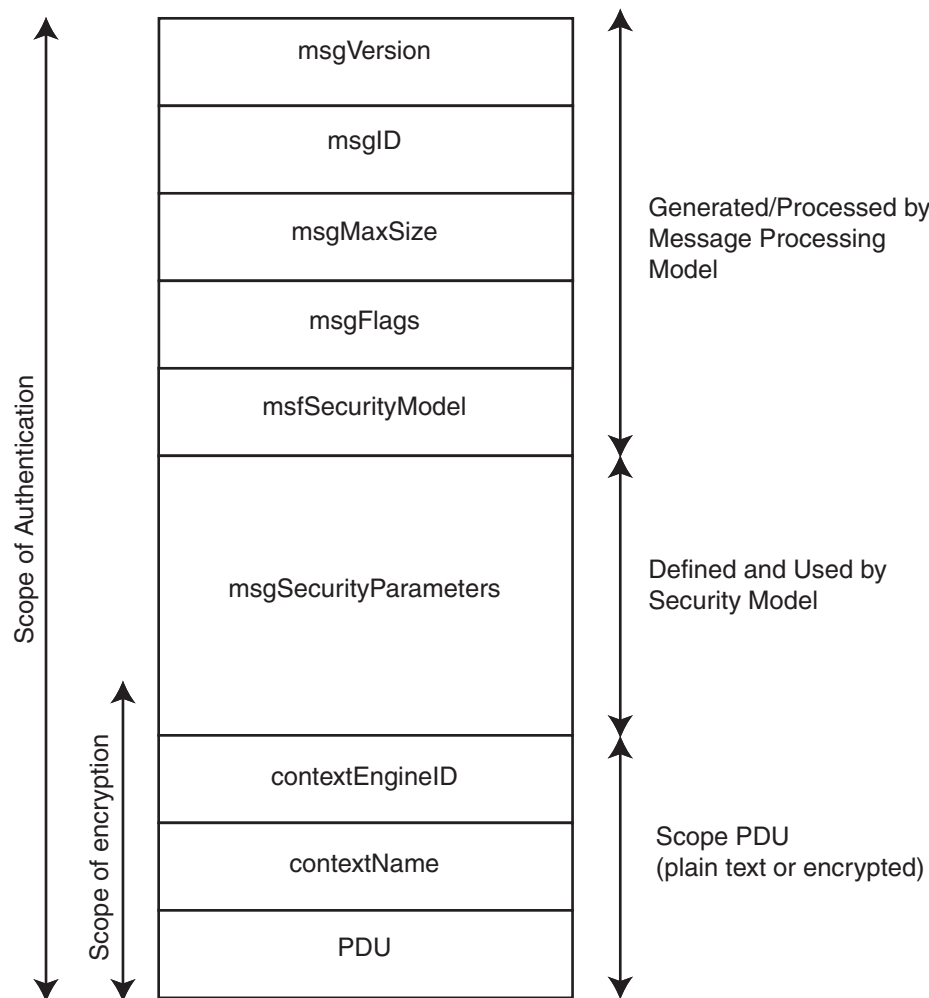
SNMPv3 builds on top of the above to provide a secure environment for the management of systems and networks. SNMPv3 covers:

- Identification of SNMP entities to facilitate communication only between known

SNMP entities (Each SNMP entity has an identifier called the `SnmpEngineID`. Each message contains `SnmpEngineID`. So SNMP communication is possible only if a SNMP entity knows the identity of its peer SNMP entity. Traps and Notifications are exceptions to this rule)

- Provision for the support for security models. A security model may define the security policy within an administrative domain or a intranet. The SNMPv3 protocol consists of the specification for the User based Security Model (USM). Definition of security goals where the goals of message authentication service includes protection against,
 - Modification of Information (Protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal)
 - Masquerade (Protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations)
 - Message Stream Modification (Protection against messages getting maliciously re-ordered, delayed or replayed in order to effect unauthorized management operations)
 - Disclosure (Protection against eavesdropping on the exchanges between SNMP engines)
- Specification for the USM security model. The USM security model consists of the general definition of different types of communication mechanisms available. They are:
 - Communication without authentication and privacy (NoAuthNoPriv)
 - Communication with authentication and without privacy (AuthNoPriv)
 - Communication with authentication and privacy (AuthPriv).
- A framework for definition of different authentication and privacy protocols. Currently the MD5 and SHA authentication protocols and the CBC_DES privacy protocols are supported in the USM.
- Definition of a discovery procedure to find the `SnmpEngineID` of a SNMP entity for a given transport address, transport endpoint address.
- Definition of the time synchronization procedure to facilitate authenticated communication between the SNMP entities.
- Definition of the SNMP framework MIB to facilitate remote configuration and administration of the SNMP entity.
- Definition of the USM MIBs to facilitate remote configuration and administration of security module
- Definition of the VACM MIBs to facilitate remote configuration and administration of the access control module.

SNMPv3 Message Format



The SNMPv3 message consists of the following fields.

msgVersion -The SNMP message version. A value of 0 means SNMPv1 message, 1 means a SNMPv2c, 2 means a SNMPv2 and 3 means a SNMPv3 message respectively. The value of message version is used to choose between the different message processing models (v1, v2c or v3) available in the SNMP engine/entity. This value is 3 for a SNMPv3 message.

The following fields are part of only the SNMPv3 message and are not available in the v1 or v2c message.

msgID - The SNMP message identifier. This is the unique ID associated with the message. The msgID field is different from the reqID field available in the PDU. It is possible that a received PDU that is part of a message cannot be decoded due to mismatch in security parameters between the SNMP entities. The msgID is used to relate the request with a response during a transaction.

msgMaxSize - The maximum size of the SNMPv3 message the requesting SNMP entity will accept.

msgFlags - The msgFlags in the SNMPv3 message contains the message security level. The bit 0 of msgFlags is used to indicate whether a message is authenticated or not. The bit 1 is used to indicate whether a message uses privacy or not. The bit 2 is used to indicate the receiving SNMP entity whether a report PDU is expected for the message. (in case the message is dropped or a response cannot be generated)

msgSecurityModel - This field indicates the security model used to generate the message. The SNMPv3 standard recommends the use of USM security model. (This field has a value of 3 when USM is used)

msgSecurityParams – An octet string that contains parameters generated by the Security Subsystem in the sending SNMP entity and processed by the Security Subsystem in the receiving entity. The Message Processing Subsystem or the Dispatcher does not interpret the contents of this string.

contextEngineID - Within an administrative domain, the contextEngineID uniquely identifies an SNMP entity that may realize an instance of a context with a particular contextName.

contextName - A contextName is used to name a context. Each contextName MUST be unique within an SNMP entity.

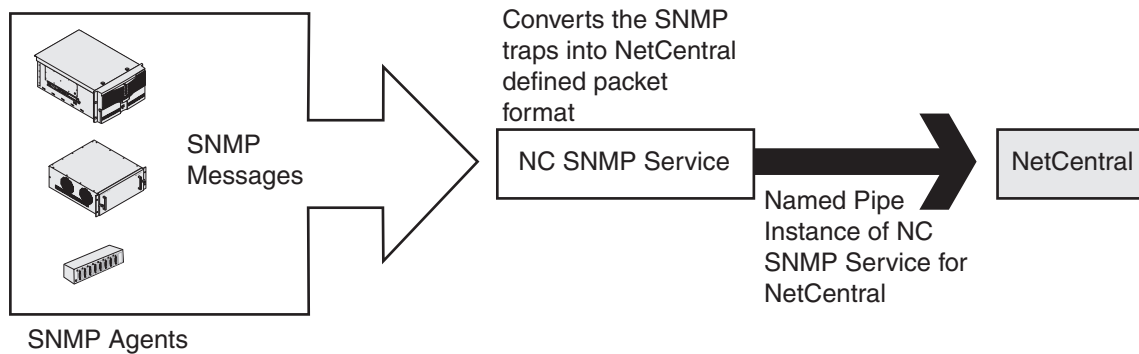
PDU - The SNMP PDU (Protocol Data Unit) used for communication between the peer SNMP entities. The SNMP request id, error status, variable bindings etc. are encapsulated in the PDU. There are different types of SNMP PDU like GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, Response-PDU, SetRequest-PDU, Trap-PDU, InformRequest-PDU, SNMPv2-Trap-PDU, and Report-PDU etc. The exact format of the PDU (the different fields inside the PDU) depends on the PDU type.

NetCentral as Trilingual Network-Management System

What is a Trilingual Network-Management System?

Trilingual network-management systems support SNMPv1, SNMPv2 and SNMPv3. To support this triple-management environment, a management application in the trilingual NMS contacts an agent. The NMS then examines information stored in a local database to determine whether the agent supports SNMPv1, SNMPv2 or SNMPv3. Based on the information in the database, the NMS communicates with the agent using the appropriate version of SNMP

Design of NetCentral SNMP Service and Communication

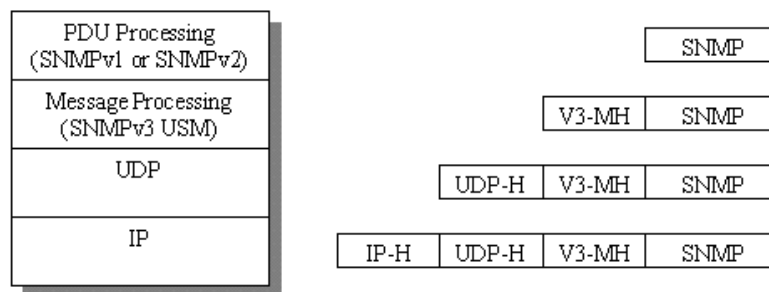


To reduce the complexity of NetCentral, a Win32 Service, which is not part of NetCentral called “NC SNMP Service”, will be running in the background and listening for SNMP traps arrive at the system on UDP port 612. If any SNMP trap arrives at the system, the “NC SNMP service” will receive and parse the packet. Then it converts the packet into NetCentral defined packet format and writes into a named pipe called “NC SNMP Named Pipe”.

NetCentral will be listening to that named pipe. Whenever, “NC SNMP service” writes into the pipe, NetCentral reads the message and displays in the Messages View.

Processing traps in NetCentral SNMP Service

Since at present NetCentral should supports only traps of all versions of SNMP, this document discusses only traps related issues as of now



A Win32 NetCentral SNMP Service will be listening for traps at UDP port number 162. If the arrived packet is a trap PDU, then the service’s *Dispatch Module* does the following tasks:

- If the arrived packet is an SNMPv3 trap, passes it to SNMPv3 Message Processing System, which does the security related processing and returns a converted SNMPv2 Trap PDU
- Now the arrived packet in the form of SNMPv2 or SNMPv1. (If it already arrived

as an SNMPv1 trap.) So the Dispatcher passes this packet for PDU processing module, which takes care of SNMPv1 and SNMPv2 trap PDUs

PDU Processing Module does the following tasks:

- Converts the received trap PDU into SNMPv2 trap PDU, if it is an SNMPv2 trap PDU.
- Check the trap OID is present in the MIB database.
- If it is present in MIB database, then it gets corresponding trap related variables from MIB database and fills the NetCentral Defined Structure

This service assumes that there is a tool available for adding and deleting MIBs with necessary *Event Definitions* and *Message Aliases* to and/or from MIB database.

What Libraries to Use?

Categories of SNMP Libraries

There are 2 categories of SNMP libraries, depends on which *standard* they follow. They are:

- WinSNMP supported Libraries.
- Open Source SNMP Libraries

Some of WINSNMP Libraries

What is WinSNMP?

WinSNMP is a Windows SNMP API specification and a standard that defines a programming interface for network management applications running under the Microsoft Windows family of GUI/operating system products, enabling those applications to make use of a logically external SNMP engine or service layer.

Some organizations have implemented WinSNMP API as commercial products such as,

- MG-SOFT Corporation implemented an SNMP engine supporting SNMPv1, SNMPv2c and SNMPv3 protocols including the complete USM security model (HMAC-MD5, HMAC-SHA, CBC-DES). The SNMP engine is programmatically accessible through the WinSNMP API. The evaluation version of the MG-SOFT WinSNMP SDK and some other MG-SOFT's WinSNMP-based SNMPv3 products (MG-SOFT MIB Browser) are available from <http://www.mg-soft.com/download.html>. An agent based on MG-SOFT's SNMP engine is available on the Internet for interoperability tests; access parameters are available on <http://www.mg-soft.com/snmpv3.html>. For more information, contact MG-SOFT WinSNMP Team.
- IBM Research has a complete multi-lingual SNMPv1/v2c/v3 stack with sample code for a Command Generator, a Command Responder, Notification Originator and Notification Receiver. The code is written in ANSI C. The code also supports the DPI (RFC1592). In addition the code contains a WinSNMP API library that allows an application to transparently talk to SNMPv1/v2c/v3 targets. For more information, contact Sara Hagggar.

- SNMPv3-enabled WinSNMP v3.0 API shipping since October 2000 to developers (via SDK product) and to end-users (via the Auto*Manage application suite). All pre-existing SNMPv1 and SNMPv2c WinSNMP applications are 100% compatible with the WinSNMP v3.0 implementation without modification or rebuilding. SNMPv3 support via addition to the WinSNMP API (constituting v3.0) is described in the Addendum (winsnmp3.htm) available at www.winsnmp.com. Applied SNMP will release its AgentX tool set (master agent and SDK) in 1Q02 with full support for SNMPv1, SNMPv2c, and SNMPv3, over WinSNMP v3.0. [Note: ACE*COMM transitioned its WinSNMP product family to a dedicated entity -- Applied SNMP -- in early 2000 for on-going support, development, and sales.]

For more information please contact Info@AppliedSNMP.com.

Some of open source Libraries and their Limitations

There are some SNMP Libraries, which are open source and free for use. Some of these libraries provide even free support also. These libraries are developed in object-oriented manner. According to these libraries design, our application can also be designed in object-oriented manner

Examples of Open Source Libraries are SNMP ++3, Net-SNMP etc

Limitation of these libraries:

If in the library any bug comes, support may not be available instantly. But since source and design documents of the library, are available with us, we can only fix the bug.

References

THE SIMPLE BOOK – Marshall T.Rose

SNMP, SNMPv2, SNMPv3 and RMON 1 and 2 – William Stallings.

RFCs: 2271, 2272, 2273, 2274, and 2275.

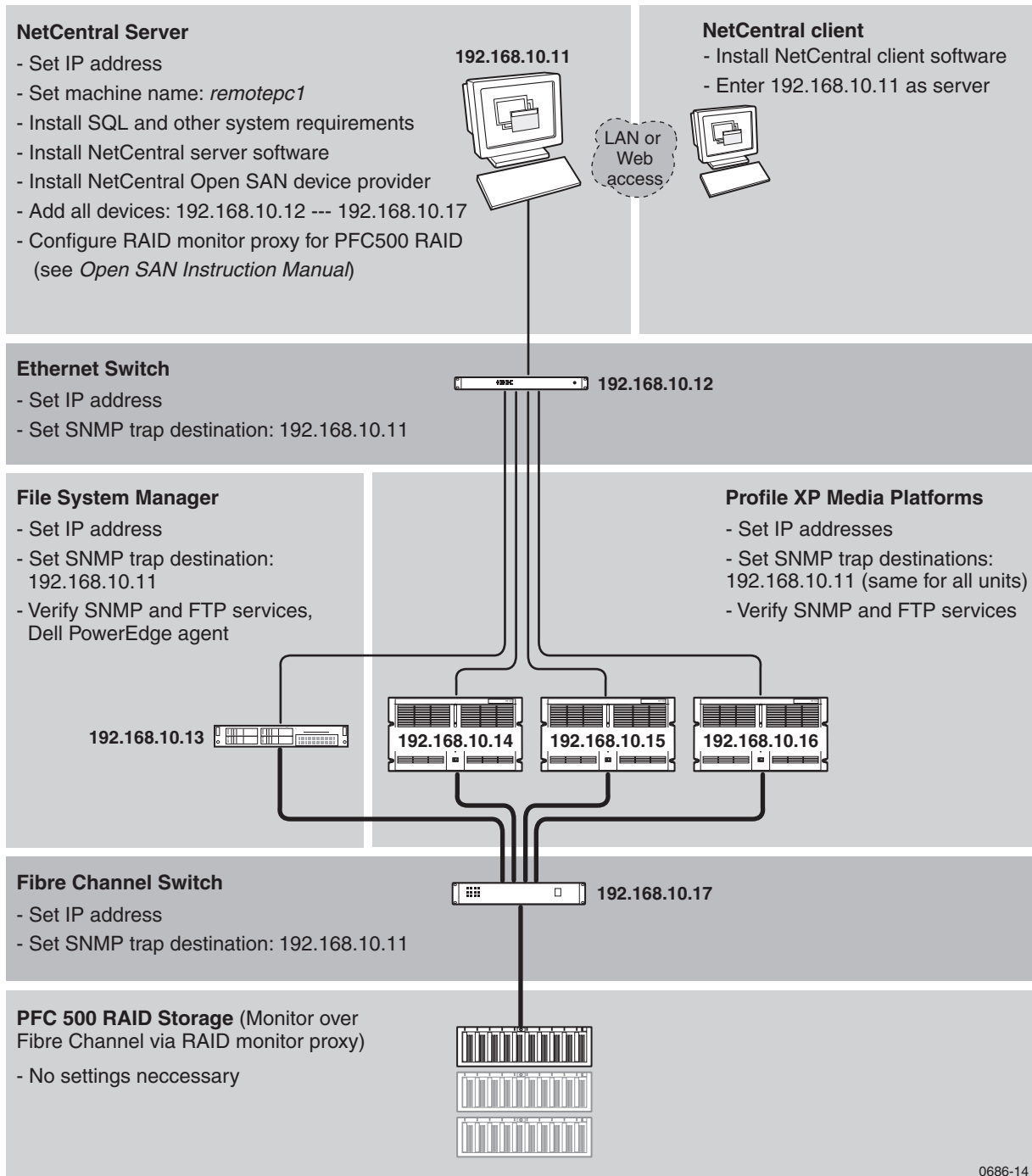
Examples of typical NetCentral systems

This section contains examples of how NetCentral can be set up to monitor some typical media devices and systems. In these examples NetCentral-related settings are specified in detail in order to illustrate how an actual system might be configured. At the same time, the media devices and systems that NetCentral monitors are represented in the simplest possible way in order to reduce unnecessary detail, so you should not use these examples as a guide to cabling or otherwise setting up the media system itself.

Use these examples to study the relationships of NetCentral components and settings so that you can understand better how to apply NetCentral to your own environment.

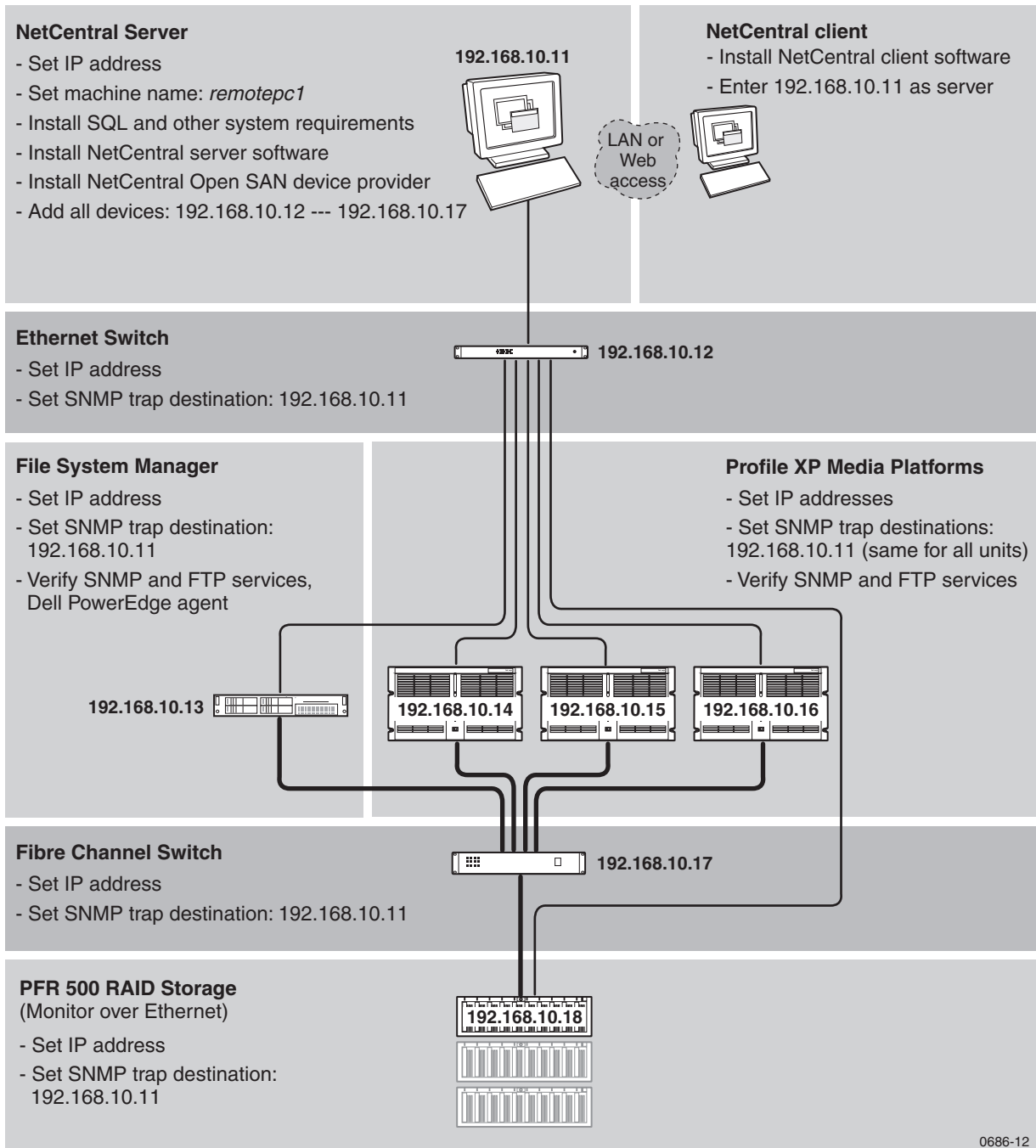
- [“Monitoring an Open SAN that uses PFC500 RAID storage” on page 162](#)
- [“Monitoring an Open SAN that uses PFR500 RAID storage” on page 163](#)
- [“Monitoring Profile XP Media Platforms” on page 164](#)

Monitoring an Open SAN that uses PFC500 RAID storage



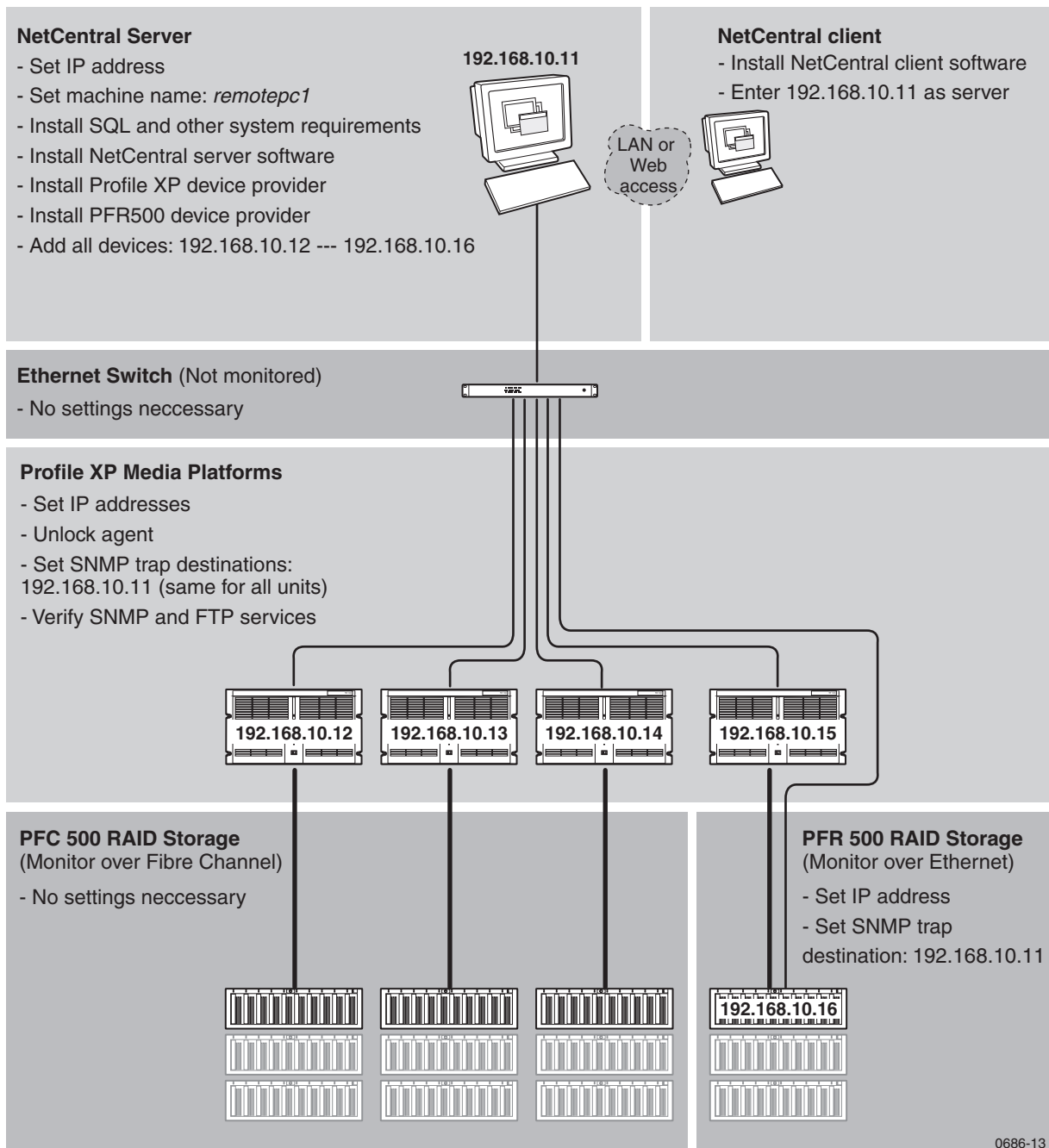
0686-14

Monitoring an Open SAN that uses PFR500 RAID storage



0686-12

Monitoring Profile XP Media Platforms



0686-13

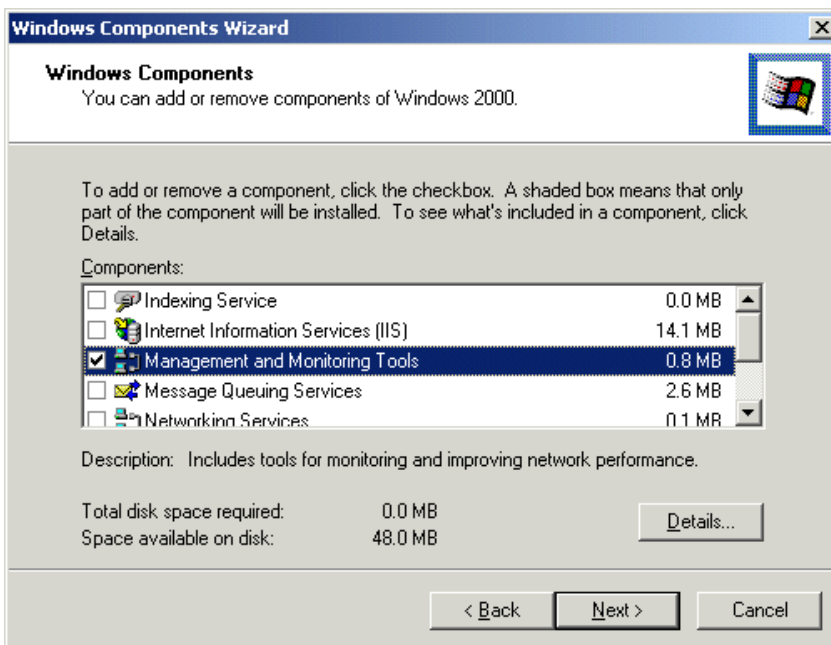
Examples of Windows procedures

Since NetCentral software supports multiple versions of Windows operating systems, several NetCentral-related tasks require that you use the version-specific documentation provided with your Windows operating system. For these tasks procedures are not provided in this manual. However, for purposes of comparison and verification, this section contains examples of procedures for some Windows operating systems. Do not execute these procedures unless you are sure they apply to the operating system on your PC.

Installing SNMP service on Windows 2000

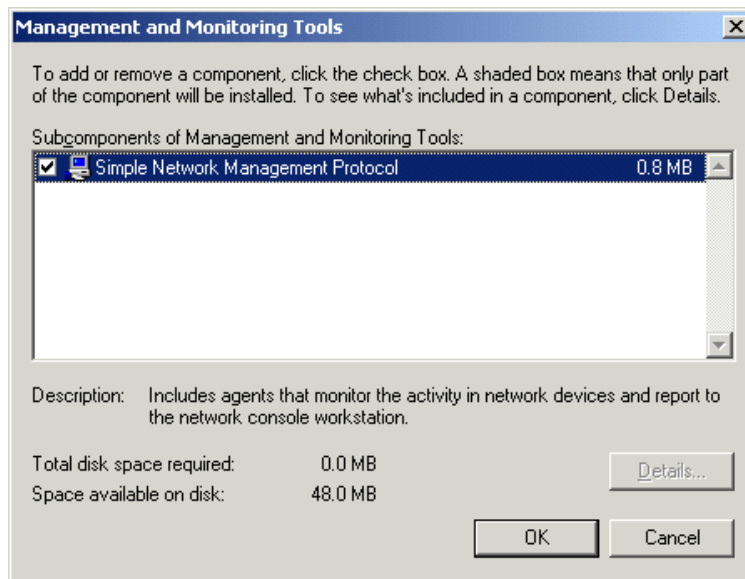
To install SNMP service on a Windows 2000 device, do the following:

1. Close all Windows programs.
2. From the Windows taskbar, click **Start | Settings | Control Panel**. The Control Panel window opens.
3. Double-click **Add/Remove Programs**. The Add/Remove Programs dialog box appears.
4. Click the **Add/Remove Windows Components** button. If you are prompted to identify your source for Windows 2000 components, insert the Windows 2000 CD-ROM or browse to the location of the components. When Windows 2000 finds your source, the Windows Components Wizard opens.



5. Select **Management and Monitoring Tools** and click **Details**. The Management and

Monitoring Tools dialog box opens.



6. If Simple Network Management Protocol is already checked, cancel and close all open dialog boxes and skip the rest of this procedure because SNMP service is already installed on your PC.
7. If not checked, select **Simple Network Management Protocol** and click **OK**.
8. On the Add/Remove Programs dialog box click **Next**. The Configuring Components screen opens and displays a progress bar while Windows 2000 installs the components.
9. When the Completing the Windows Components Wizard screen appears, click **Finish**.
10. Click **Start | Settings | Control Panel**, open **Administrative Tools** and in **Services** verify that SNMP Service and SNMP Trap Service appear in the list.

Setting SNMP trap destinations on Windows 2000

This procedure is an example of how you set trap destinations on a monitored device that runs the Windows 2000 operating system.

1. From your Windows taskbar, click **Start | Settings | Control Panel**. The Control Panel window appears.
2. Double-click **Administrative Tools** and then double-click **Computer Management**.
3. In the console tree, expand **Services and Applications** and click **Services**.
4. In the details pane, click **SNMP Service**.
5. On the **Action** menu, click **Properties**.
6. On the **Traps** tab, under Community name, type `public` or some other case-sensitive community name to which this computer will send trap messages,

and then click **Add to list**.

7. In Trap destinations, click **Add**.
8. In Host name, IP or IPX address, type the IP address or name of the NetCentral server, and click **Add**.
9. Repeat steps six through eight until you have added communities and trap destinations for all the SNMP managers that monitor the device.
10. On a Windows 2000 monitored device these SNMP changes take effect immediately. The SNMP service does not need to be restarted for your settings to take effect.

Glossary

Action

A process that the NetCentral server PC executes, such as beeping, that is directed by the NetCentral software as a result of a change in status on a device.

Action provider

A software module that defines and controls an action, such as sending e-mail, that can be triggered by the NetCentral system. A new action provider can be plugged in to an existing NetCentral system. Each action provider is a file, such as *Mail.dll*.

Actions view

The Actions view button in the left-panel portion of the NetCentral interface displays lists of currently configured actions for the selected folder, device, or subsystem.

Active Drawings

A technology NetCentral uses, especially for HTML page features in the Facility view.

Agent

The software component that resides on a managed device and provides the required interface to SNMP.

Application logs

Logs of NetCentral software events. These events have to do with the software itself, rather than the devices being monitored by the software.

Auto-Discovery

The process used by the NetCentral software to check a range of user-configurable IP addresses, search for NetCentral compatible devices, and add such devices to the NetCentral system as they are found.

Community name

A parameter defined by SNMP by which devices can be grouped for the purpose of controlling the flow of management information.

Critical

The highest level of severity for a NetCentral message. An critical message is sent when a device has ceased to operate or is currently operating with severely hampered functionality.

Device

A piece of hardware.

Device provider

A software module that enables a particular type of device, such as a QLogic Fibre Channel switch, to be included in the NetCentral system. A new provider can be plugged in to an existing NetCentral system. Each provider is a file, such as *SilkWormProvider.dll*.

DHCP

Dynamic Host Configuration Protocol, an auto-configuration service that allows a machine to obtain an address without prior knowledge at boot time.

Discovery process

The process used by the NetCentral software to add devices. This same process is used when a user adds a device manually and when the software adds a device automatically via Auto-Discovery.

Dynamic IP address

An IP address assigned dynamically to a machine by a DHCP server.

Element

A NetCentral term that is used to refer to any SNMP managed entity. In the NetCentral system an element is the same as a device.

Element provider

The Grass Valley engineering term for device provider.

Facility view

The Facility view button in the left-panel portion of the NetCentral interface displays subsystem properties and HTML pages associated with folders.

Fibre Channel

A general set of integrated standards developed by ANSI for flexible information transfer over multiple physical interface types.

Graphs view

The Graphs view button in the left-panel portion of the NetCentral interface displays charts of statistical information about status messages received from monitored devices.

Heartbeat polling

Messages sent periodically by the NetCentral software that check the “heartbeat” of monitored devices by requesting the devices to respond.

HTTP

Hypertext transfer protocol — the protocol by which Web (HTML) pages are communicated

Informational

The lowest level of severity for a NetCentral message. Sent when a device has experienced a change in status within normal operating parameters.

Management information base (MIB)

A hierarchical collection of information about a managed element in a format standardized by SNMP.

Manager

The software component that resides on the NetCentral server and provides the required interface to SNMP. NetCentral server

Messages view

The Messages view button in the left-panel portion of the NetCentral interface displays lists of status messages for the currently selected folder, device, or subsystem.

NetCentral server

The PC on which the NetCentral server software is installed and used to monitor devices.

NetCentral software

The software modules, installed on a NetCentral server and on NetCentral clients, that provide the primary functionality to the NetCentral system.

NetCentral system

The entirety of the components associated with monitoring devices, including NetCentral servers, NetCentral clients, devices, NetCentral client via Web access, and the network.

Offline

Something not active or not available for access in a system.

Panel

A portion of an interface window. Panels are usually separated by dividing bars.

Point-to-point

A scheme for connecting two computers over a telephone line or over a network link that acts like a telephone line.

Port

An access point in a device where a link attaches.

Protocol

A convention for data transmission that defines timing, control, format, and data transmission.

Reset

A low level of severity for a NetCentral message. Sent when a device returns to normal operating parameters after a critical or warning level condition is resolved.

Service pack

Software that is intended to add extended functionality and fix problems with existing software.

Simple Network Management Protocol (SNMP)

The protocol defined by the Internet Engineering Task Force (IETF) to facilitate the exchange of management information between networked devices.

Simple Mail Transfer Protocol (SMTP)

The protocol used to send Internet e-mail.

Static IP address

An IP address that is assigned to a machine on an IP network manually by a system administrator.

Status indicator

An icon, text message, or system action propagated by the NetCentral system for the purpose of communicating to the user some information about the status of a device.

Subsystem

A logical, defined portion of a device's functionality for which management information is captured and reported through the NetCentral system.

Subsystem view

That portion of the NetCentral interface that displays the subsystems of a particular type of device and the current status of each of the subsystems of the selected device.

System tray

A portion of the Windows operating system taskbar reserved for icons representing background processes currently active on the machine.

Threshold condition

A measurable point in the functionality of a device subsystem, beyond which the subsystem is deemed to have changed status.

Trap

The unsolicited SNMP message that a device sends when it experiences a change in status.

Virtual Web server directory

A mapping of a short name or alias to the physical directory on a Web server. The physical directory contains the hypermedia that a Web browser can access using the short name.

Warning

The medium level of severity for a NetCentral message. A warning message is sent when a device has a reduced ability to function and may fail soon, but at the current moment it is still operating within specifications as designed.

Index

A

- access rights
 - in NetCentral 113
 - logon to NetCentral manager 47
 - to NetCentral features 114
- action providers
 - defined 19
 - device-specific 99
 - functionality in NetCentral software 18
 - plugging in 99
- actions
 - Beep 95
 - cancelling 64
 - configuring 87
 - configuring default properties 91
 - defined 84
 - filtering by device 100
 - filtering by folder 101, 102
 - interacting with messages 84
 - Launch URL 98
 - Play Audio 94
 - preparation before adding 87
 - Run Program 96
 - Schedule Mail 91
 - Send Mail 91
 - sound card needed 94
 - testing 92
- Actions view 54
- Actions wizard 87
- active drawings 23
 - removing devices from HTML page 109
- adding
 - devices 104, 105
 - folders 55
- Adding an action for a message 89
- administrator
 - log-in privileges 25, 31, 33
 - logon to NetCentral 47
 - permissions in NetCentral 113
- alarms
 - allowing time before triggering 112
 - clearing 64
 - defined 60
 - resetting state 65
 - see also* actions
- alerts, *see* alarms, warnings

- annotation layer 142
- Application Logs Viewer 104
- architecture, of NetCentral software 18
- assign groups to users 113
- audio, *see* Play Audio action
- Auto-Discovery
 - adding devices with 106
 - at first startup 37
 - defined 105
 - restoring defaults 130
 - starting 37
 - turning off 108

B

- Beep action
 - configuring 95
 - turning off 64

C

- cell phone notifications 92
- checklist
 - NetCentral, installing and setting up 27
- Ciprico, *see* PFR500
- clearing alarms 64
- client
 - architecture 18
 - installing software 32
 - remote access 48
 - requirements 29
- command line arguments 96
- command prompt, for finding IP address 29
- community, *see* SNMP community
- connectors
 - adding on HTML page 137
- contact information for a device 68
- copying messages 86

D

- Dead or off-line message 60
- device list 66
- device provider
 - defined 19
 - functionality 18
 - installing software 33
 - registration 130

- verifying installation 35
- devices
 - adding 41, 104, 105
 - copying into a folder 56
 - finding 66, 72
 - grouping and arranging 55
 - messages initiated by 84
 - parameters for threshold conditions on 85
 - removing 108
 - removing from HTML page 109
 - using device-specific applications 82
- device-specific logs 79
- DHCP server 29
- diagnosing NetCentral problems 124
- dialog boxes
 - Add Device 41, 105
 - Auto-Discovery 106, 110
 - Auto-Discovery Settings 107
 - Beep Configuration 95
 - Create Shortcut 49
 - Download Device Logs 80
 - E-mail Configuration 92
 - E-mail Schedule Configuration 93
 - Filter Messages 100, 101, 102
 - Folder properties 55
 - Mail Schedule List Configuration 93
 - Play Audio Configuration 94
 - Run Program Configuration 96
 - System Settings 106, 110, 112
- disabling actions 100
- downloading device-specific logs 80
- Dynamic Host Configuration Protocol (DHCP) 29

E

- e-mail, *see* Send Mail action, Schedule Mail action
- examples
 - monitoring a PFC500 Open SAN 162
 - monitoring a PFR500 Open SAN 163
 - monitoring Profile XP Media Platform 164

F

- Facility view 52
 - folders 55
 - graphical view 57
- Filter Message wizard 101, 102
- filtering messages 100
- finding monitored devices 66, 72

- folders
 - adding 55
 - copying devices into 56
 - embedding in HTML page 142
 - Facility view 55
- folders, adding 55
- FTP, on Profile XP and FSM 42

G

- graphical view
 - in Facility view 57
- graphs
 - defining type and time period 78
 - researching 77
- Grayed-out text, interpreting 39, 61
- groups
 - assigning for security 113

H

- heartbeat polling, configuring 111
- HTML page
 - annotation layer 142
 - background 57
 - embedding a folder icon 142
 - removing devices 109
 - subsystem connectors 137
- HTML page, *see* graphical view
- Hypertext Markup Language (HTML) 22, 23

I

- icons
 - as status indicators 60
 - status 60
 - system tray 62
- indicators, status 60
- installing software
 - client 32
 - device provider 33
 - server 31
- Internet Engineering Task Force (IETF) 21
- Internet Protocol (IP)
 - address as trap destination 40
 - address of NetCentral server 29
 - addresses of monitored devices 105
 - dynamic addresses 29
 - range of addresses for Auto-Discovery 107

K

keep-alive function 112

L

licensing

- testing NetCentral software components for 124
- violations 130

Light colors, defined 61

log-in

- administrator privileges 25, 31, 33, 129
- initial start of NetCentral 36
- to Netcentral 113

logs

- accommodating size increases 118
- application logs viewer 104
- defined 128
- device-specific 77
- downloading from devices 80
- NetCentral 128

M

management information base (MIB) 21

Managing port access 116

message boxes

- Delete device 42, 108
- Network Connection 41, 106

messages

- acknowledged displayed 70
- adding remarks 85
- copying 86
- dead or off-line 60
- defined 84
- definitions of status levels 60
- exporting 73
- filtering by device 100
- filtering by folder 101, 102
- finding 72
- in the NetCentral window 63
- interacting with actions 84
- number displayed 70
- printing 76
- querying 75
- researching 69
- responding to 63
- suggestions for corrective actions 61
- time period displayed 70
- viewing a list of all possible 127

Messages view 53

- arranging 71

N

name resolution on a network 105

NCAAdministrator group for NetCentral security 113

NCTechnician group for NetCentral security 113

NCUser group for NetCentral security 113

NetCentral Lite

- detects local XP only 130
- documentation for 12
- installing 12
- using 12

NetCentral log

- using 128

NetCentral software

- architecture 18
- automatic startup 49
- core 19
- installing 31, 32
- plugins 19
- starting 37
- troubleshooting 123

NetCentral window

- viewing 50

networks

- defined as managed by SNMP 21
- name resolution 105
- settings that affect performance 108, 112

notifications

- see also* actions
- configuring 87
- customized sets 84
- multiples of the same type 87

O

Open SAN

- FTP for log downloads 42
- monitoring a PFC500 system 162
- monitoring a PFR500 system 163

Open SAN, *see* Open SAN

open view in new window 54

operating system

- requirements 28

P

- pager notifications 92
- PFR500
 - monitoring a Open SAN that uses 163
 - monitoring a Profile XP Media Platform that uses 164
- Play Audio action
 - configuring 94
 - sound card needed 94
- port access 116
- privileges, administrator-level 25, 31, 33
- problems
 - at Windows NT startup 129
 - with the NetCentral system 123
- Profile XP Media Platform, example of
 - monitoring 164
- protocols
 - multiple in NetCentral 42
- public, defined as SNMP community 22

Q

- querying NetCentral messages 75

R

- refreshing the information area 54
- registered component, testing for 124
- re-installing, Windows NT Service Pack 129
- remarks
 - added to messages 85
- remote access to NetCentral 48
- removing devices 108
- reports, NetCentral software diagnostic 125
- requirements
 - facility 28
 - NetCentral client 29
 - NetCentral server 28
 - NetCentral system on a network 28
- researching
 - messages 69
- reset messages, defined 60
- reset state 65
- Run Program action
 - configuring 97

S

- Schedule Mail action
 - configuring 91

- search
 - for device 66
 - for folder 56
 - for messages 72
- security
 - administrator privileges 25, 31, 33
 - NetCentral 113
- Send Mail action
 - configuring 91
- server
 - architecture 18
 - dangers of dynamic IP addresses 29
 - installing software 31
 - requirements 28
- Service Pack, *see* Windows NT Service Pack
- shortcuts, creating in Windows NT startup 49
- Simple Mail Transfer Protocol (SMTP) 92
- Simple Network Management Protocol, *see* SNMP
- SNMP
 - agent 130
 - community, as trap destination 40
 - configuring community name 105
 - configuring properties 40
 - definitions
 - agent 21
 - community 22
 - managed device 21
 - managed networks 21
 - management information base (MIB) 21
 - management stations 21
 - manager 21
 - SNMP 21
 - traps 22
 - function of trap destinations 22
 - restarting services 38
 - trap service 131
 - trap target, trap recipient 40
 - tutorial 143
- SNMP trap configuration
 - at first startup 37
 - manually setting trap destinations on monitored devices 39
- SNMP trap messages
 - definition 37
 - verifying 39
 - viewing a list of all possible 127
- software
 - client 32

- device provider 33
- reinstalling 33
- server 31
- uninstalling 33
- sound card
 - needed for Play Audio action 94
 - verifying on a PC 131
- sounds, stopping 64
- startup
 - creating shortcuts 49
 - problems with 129
- status indicators
 - interpreting 60
- status information, viewing 67
- status levels defined 60
- stopping NetCentral 48
- stopping sounds 64
- subsystem connectors
 - adding on HTML page 137
- support
 - for Grass Valley products 13
 - phone 13
 - Profile Users Group 13
 - Web 13
- Syslog monitoring 42
- system settings
 - Auto-Discovery 106, 110
 - heartbeat polling 112

T

- testing
 - beep action 96
 - e-mail action 92
 - for registered/licensed NetCentral software component 124
 - play audio action 95
 - run program action 97
- threshold conditions, setting parameters on devices 85
- trap engine 129
- traps, *see* SNMP traps
- Tree view
 - arranging 55
- turning off audible alarms 64

U

- U.S. Windows version, requirements 28
- URL, launching as action 98

- user groups
 - in Windows and NetCentral 113
- user permissions in NetCentral 113

V

- version information 82
- views
 - Actions 54
 - Facility 52
 - Graphs
 - graphical view 53
 - in multiple windows 54
 - Messages 53
 - NetCentral main window 51
 - Tree view 55

W

- warning, defined 60
- wave file (WAV)
 - defined 94
 - playing as an action 95
 - turning off sounds 64
- Web browser, *see* browser
- Web page, defined 23
- Wide Area Network (WAN), Auto-Discovery
 - within 107
- Windows
 - requirements 28
- Windows NT Service Pack
 - problems if not re-installed 129

