Nortel Communication Server 1000

Communication Server 1000 Fault Management — SNMP

NN43001-719

Document status: Standard
Document version: 02.02
Document date: 7 December 2007

Copyright © 2007, Nortel Networks
All Rights Reserved.

Sourced in Canada

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.
All other trademarks are the property of their respective owners.

Contents

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Procedures

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

New in this release

The following sections detail what’s new in *Communication Server 1000 Fault Management — SNMP (NN43001-719)* for release 5.5.

- "Features" (page 7)
- "Other changes" (page 7)

Features

See the following sections for information about feature changes:

Rated call capacity

A detailed description of the use of rated call capacity in the hrProcessorLoad diagnostic is added for Release 5.5. For more information see hrProcessorLoad, page 74.

Disk drive monitoring threshold points

Release 5.5 contains a list of space utilization thresholds for various disk drives. For more information see Space utilization thresholds, page 72 .

Other changes

See the following sections for information about changes that are not feature-related:

Revision history

December 7, 2007	Standard 02.02. This document is up-issued to support Communication Server 1000 Release 5.5. This document provides a description of rated call capacity (hrProcessorLoad, page 74) and a list of space utilization thresholds (Space utilization thresholds, page 72).
December 7, 2007	Standard 02.01. This document is up-issued to support Communication Server 1000 Release 5.5.
September 2007	Standard 01.04. This document is up-issued to document how to setup SNMP from a MGC card.

Copyright © 2007, Nortel Networks

July 2007	Standard 01.03. This document is up-issued for changes to QOS MIB Access setup.
June 2007	Standard 01.02. This document is up-issued to remove the Nortel Networks Confidential statement.
May 2007	Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0. This document is renamed *Communication Server 1000 Fault Management — SNMP (NN43001-719)* and contains information previously contained in the following legacy document, now retired: *Simple Network Management Protocol: Description and Maintenance (553-3001-519)*. In addition, all references to adminGroup2 and adminGroup3 community strings in the section "Community strings" (page 39) are changed to admingroup2 and admingroup3. to reverse previous changes. The syntax was correct initially and should have remained. The admingroup syntax is all lower case.
July 2006	Standard 4.00. This document is up-issued for changes in technical content. All references to admingroup2 and admingroup3 community strings in the section "Community strings" (page 39) are changed to adminGroup2 and adminGroup3. The community strings are case sensitive and do not work if they are entered in all lower case. The syntax for Community Name and User group are reversed in "Call Server default community strings" (page 39) and "Signaling Server, Voice Gateway Media Card, and MGC default community strings" (page 40). The community strings are in brackets and not the User Group.
January 2006	Standard 3.00. This document is up-issued with changes to configure SNMP trap destinations. Configuring the required ELAN routing entries and the SNMP trap destination subnet mask is updated to 255.255.255.255.

Copyright © 2007, Nortel Networks

August 2005	Standard 2.00. This document is up-issued to support Nortel Communication Server 1000 Release 4.5.
September 2004	Standard 1.00. This document is issued to support Simple Network Management Protocol (SNMP) capabilities for Nortel Networks Communication Server 1000 Release 4.0 and Meridian 1 systems.

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

How to get help

This chapter explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation is current at the time the product is released. To check for updates to the latest documentation for Communication Server (CS) 1000, go to www.nortel.com and navigate to the Technical Documentation page for CS 1000.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:
www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835). Outside North America, go to the following Web site to obtain the telephone number for your region:
www.nortel.com/callus

Copyright © 2007, Nortel Networks

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to: www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Copyright © 2007, Nortel Networks

Introduction

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

ATTENTION

Setup and use of Simple Network Management Protocol (SNMP) and Network Management Systems (NMS) for alarm monitoring requires knowledgeable technical staff with appropriate experience. For most Network Management Systems, it is necessary to import the Nortel Communications Server 1000 or Meridian 1 Management Information Bases (MIB) and perform configuration changes to support the system alarms.

Some systems require limited application work using the development kit provided with the Network Management System. Contact the Network Management System provider if assistance is required.

Subject

This document describes the Simple Network Management Protocol capabilities in terms of the Call Server, Signaling Server (SS), Voice Gateway Media Cards (VGMC), Media Gateway Controller (MGC), Network Routing Service (NRS), and Enterprise Common Manager (ECM). It describes how SNMP is configured, and how it operates to allow the management system to receive management information about the system components.

See *IP Trunk Description, Installation, and Operation (NN43001-563)* and *Survivable Remote Gateway Configuration Guide (NN42120-501)*, for information about the IP Trunk MIB and SNMP capabilities for IP Trunk and Survivable Remote Gateway (SRG).

Note about legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000, Release 5.5 software. For more information about legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page:

Copyright © 2007, Nortel Networks

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

For more information, see one or more of the following NTPs:

- *Meridian 1 PBX Option 11C Cabinet and Chassis Software Upgrade (NN43011-459)*
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview (NN43021-458)*
- *Communication Server 1000E Upgrade Procedures Overview and Introduction (NN43041-458)*

Conventions

The following sections describe the conventions used in this document.

Terminology

In this document, the following systems are referred to generically as *system*:

- Meridian 1
- CS 1000

The following systems are referred to generically as *Small System*:

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as *Large System*:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Copyright © 2007, Nortel Networks

- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Network Routing Service Installation and Commissioning (NN43001-564)*
- *Converging the Data Network with VoIP (NN43001-260)*
- *Telephony Manager 3.1 Installation and Commissioning (NN43050-300)*
- *Telephony Manager 3.1 System Administration (NN43050-601)*
- *IP Peer Networking Installation and Commissioning (NN43001-313)*
- *IP Trunk Description, Installation, and Operation (NN43001-563)*
- *IP Line Fundamentals (NN43100-500)*
- *Software Input/Output System Messages (NN43001-712)*
- *Software Input/Output Maintenance (NN43001-711)*
- *Communication Server 1000M and Meridian 1 Small System Maintenance (NN43011-700)*
- *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*
- *Communication Server 1000E Maintenance (NN43041-700)*
- *Installing Nortel Enterprise Network Management System (321537-B)*
- *Administering Nortel Enterprise Network Management System (205969-J)*
- *Using Nortel Enterprise Network Management System (207569-G)*

Online

To access Nortel documentation online, click the Technical Documentation link under Support & Training on the Nortel home page:
www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

SNMP system capabilities

Contents

This chapter contains information about the following topics:

SNMP terminology

Event – an occurrence on the system that causes a change in status on a device or system component which can trigger a log message and a corresponding message/trap.

Alarm – a message notification (for example, SNMP trap or system message) that indicates a fault on the device. The alarm may or may not represent an error in the system.

Fault – an event that is abnormal and undesirable, and can affect service. Generally faults require some type of intervention or corrective action. Faults that require corrective action are sent as alarms. Although the term fault usually refers to hardware and the term error usually refers to software, you can use these terms interchangeably.

Copyright © 2007, Nortel Networks

community string – an access mechanism in SNMP agents that provides management systems read-only or read/write access to system data. An agent does not accept requests from a management system that does not use a valid community string.

Report - describes some of the operational traits of a network.

System message – a message that is sent from the system when an event occurs. All system messages can be sent through a serial port. Most, but not all, system messages also result in the generation of traps. These messages usually are given an identifier in the format XXXnnnn or XXXXnnnn, where X is an alphabetic character and n is a number from zero to nine (for example, AUD0001). For more information about system messages, see *Software Input/Output System Messages (NN43001-712)*.

Trap – a one-way notification sent from the SNMP agent on a device to the Network Management System (NMS) when a specific condition occurs, such as the failure of a system component. In Nortel CS 1000 products, the traps are sent in the form of an SNMP V1 TRAP-TYPE Protocol Data Unit (PDU). The PDU type is TRAP-V1, and the trap type is Enterprise-Specific.

Agent – SNMP agent software running on any intelligent device (for example, a PC or router). An agent receives requests from a management system. It also can act as a watchman and initiate traps when a specific event occurs or a threshold is reached.

MIB – Management Information Base. A MIB is a set of objects that represent different kinds of management-related information about a network device. It can be considered a database of information about a device that is accessible through an agent. A MIB Module describes the objects (entries) that are to be included in the agent database. MIB objects must be defined as to which objects are available, the object names and types, and the related values. This information is included in a MIB Module.

MIB Module – a file used by the management system to understand the structure of the MIB database (and/or the traps) on the device. A MIB Module also can contain the information that defines the structure of the traps sent from the device. In many cases, the MIB Module is simply referred to as a MIB.

Management system – a system that is used to manage devices in a network. In the case of an SNMP management system, the system may send requests to the device agents and receive traps from the network devices. A management system can initiate the *get*, *getNext*, and *set* operations.

Copyright © 2007, Nortel Networks

`getRequest` command – an SNMP request from the management system to the agent for a specific object in the MIB.

`getNextRequest` command – a request for the next object in the MIB.

`getResponse` command – used by the queried agent to fulfil the request made by the management system.

`setRequest` command – a request from the management system to the device agent to change the value of a parameter in the MIB.

Overview

Simple Network Management Protocol (SNMP) is part of the Transport Control Protocol/Internet Protocol (TCP/IP) suite. The SNMP architecture consists of management systems and agents. SNMP provides the ability to monitor devices and communicate their status information (when requested or when an event occurs) to designated locations on a TCP/IP network.

SNMPv1 and SNMPv2 are supported for querying elements on the network, SNMPv1 is supported for trap generation, and SNMPv2C is supported for the MIBs.

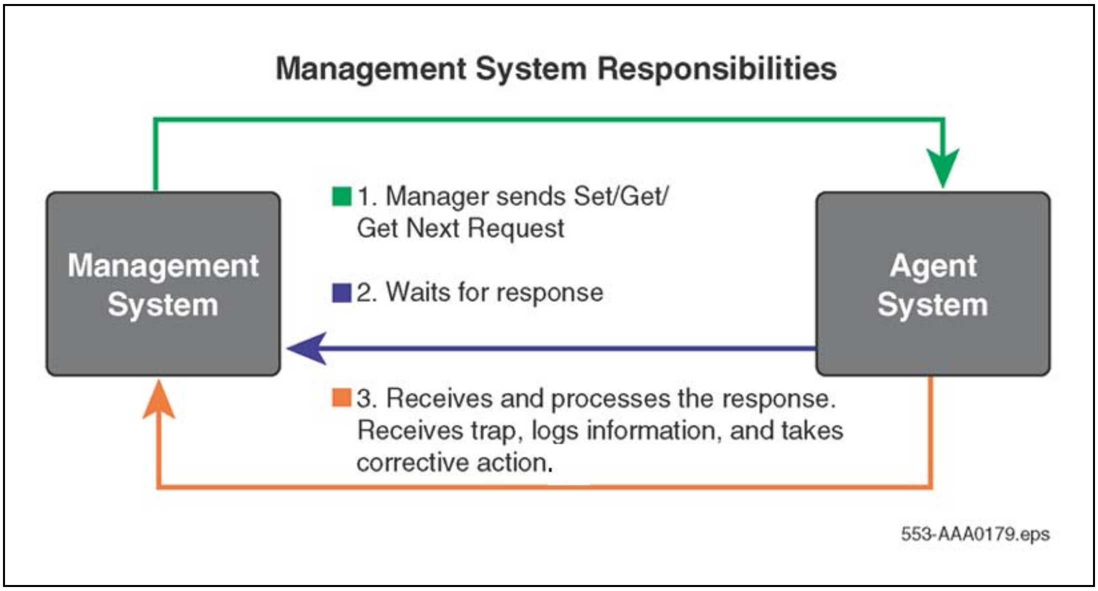
SNMP provides for the collection and manipulation of network information. It gathers information by the following methods:

- from traps sent by the devices
- by polling the devices on the network from a management system at fixed or random intervals. See "Management system responsibilities" (page 20).

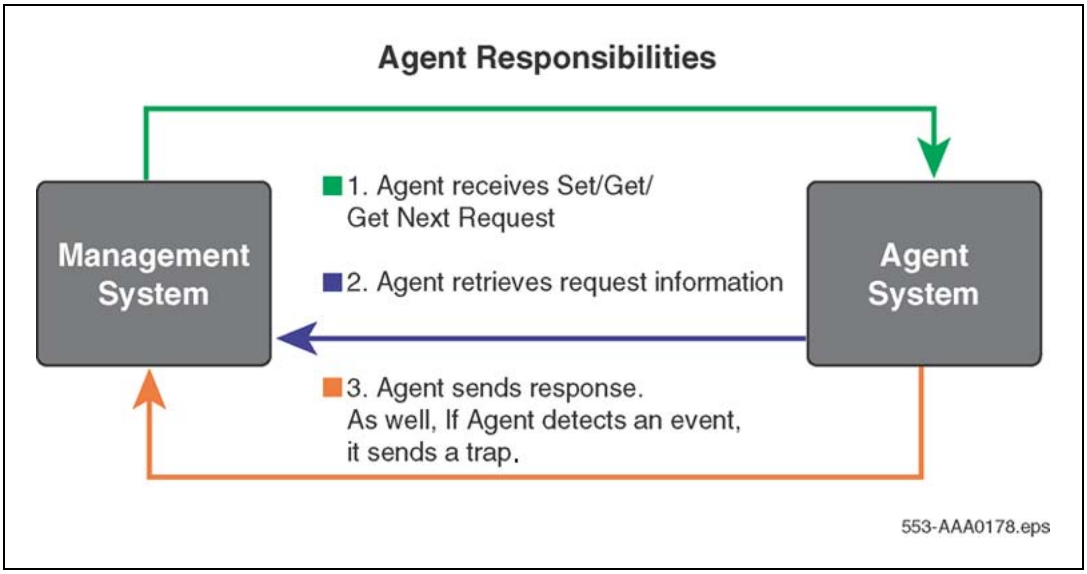
  When the request is received, the agent on the device returns the requested data. See "Agent responsibilities" (page 20).

Copyright © 2007, Nortel Networks

Management system responsibilities


Management System Responsibilities
Management System
Agent System
🟩 1. Manager sends Set/Get/ Get Next Request
🟦 2. Waits for response
🟧 3. Receives and processes the response. Receives trap, logs information, and takes corrective action.
553-AAA0179.eps

Agent responsibilities


Agent Responsibilities
Management System
Agent System
🟩 1. Agent receives Set/Get/ Get Next Request
🟦 2. Agent retrieves request information
🟧 3. Agent sends response. As well, If Agent detects an event, it sends a trap.
553-AAA0178.eps

SNMP capabilities

To understand how SNMP operates on a system running CS 1000 software, it is important to be aware that a number of device components have embedded SNMP agents. The device components are:

- Call Servers
- Signaling Servers
- Voice Gateway Media Cards

Copyright © 2007, Nortel Networks

- Media Gateway Controllers (MGC)
- Network Routing Service (NRS)
- Enterprise Common Manager (ECM)

Although the devices each contain specific SNMP agents, they all support the COMMON-TRAP-MIB.mib, which means that traps sent from each device agent are in the same format. CallPilot and Contact Center also have SNMP capabilities that are described in their respective technical documentation.

All traps sent from the devices originate as events that trigger system messages. Except for Service Change (SCH) messages, approximately 80 percent of system messages are also sent as traps. System messages can be sent through the serial port of the component to a receiving system, or they can be sent as traps by the SNMP protocol through an IP network to a receiving SNMP management system, such as Telephony Manager (TM) or a third-party SNMP Management System.

The Call Server sends most of the system message categories, which range from the ACD type to the XMI type. The Call Server can suppress messages or traps below a specified priority and alter the individual message or trap severity through the Event Preferences Table.

Few trap message types are sent from the Signaling Server and the Voice Gateway Media Card devices. The traps are primarily ITG, ITS, QOS, or WEB message types.

> ***Note:*** See the "List of terms" (page 111) for a description of the trap message types.

System SNMP architecture

Some system devices (Call Server, NRS, ECM) have their own specific SNMP agent with different architecture, whereas other devices have the same architecture (Signaling Server, Voice Gateway Media Card, MGC). The following sections describe the architecture for each device.

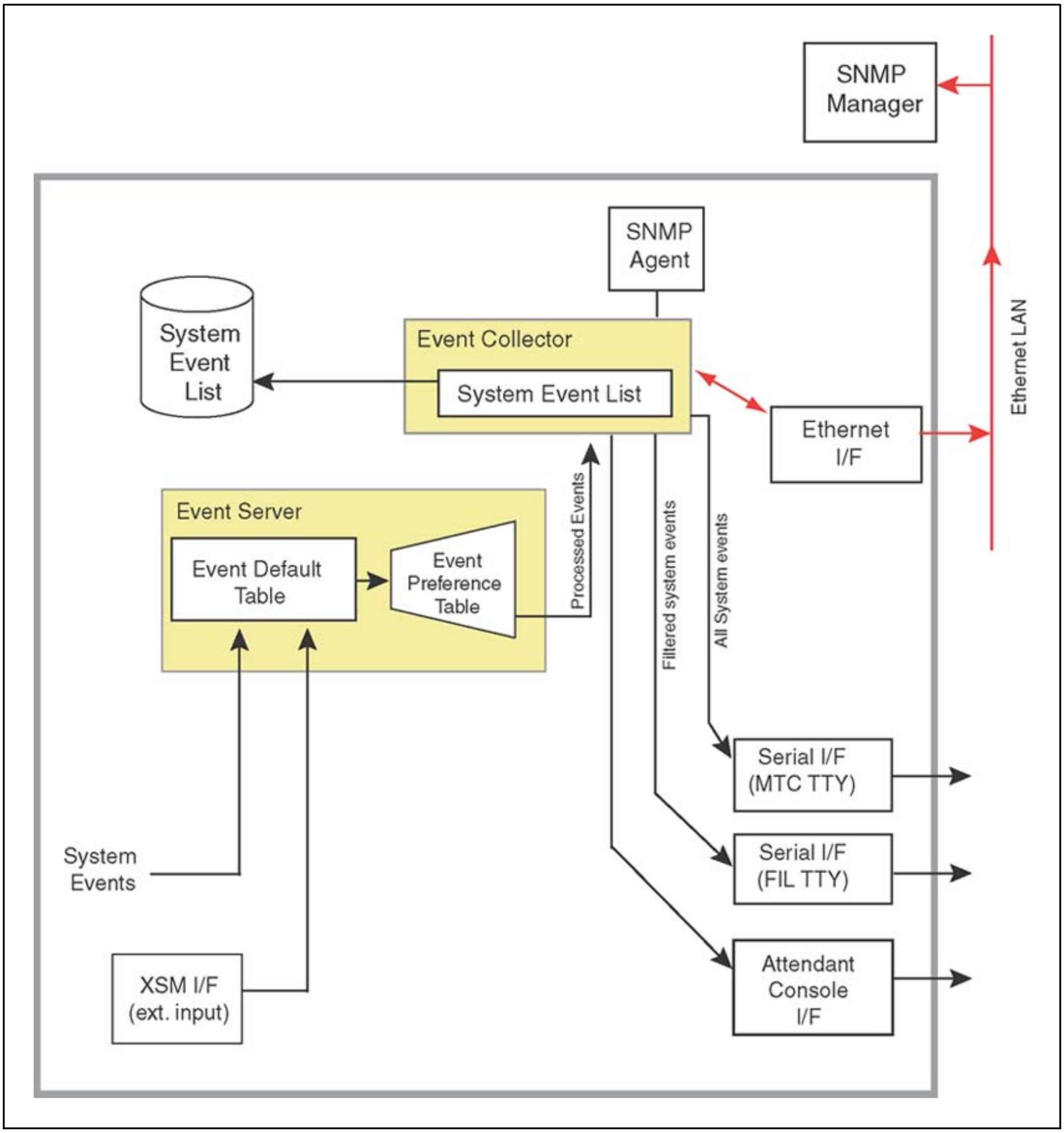
> ***Note:*** In this document, the term *Call Server* also encompasses the SNMP capabilities of the Meridian 1 core.

Call Server architecture

Call Server architecture contains the Event Server and Event Collector. See "Event architecture on the Call Server" (page 22).

Copyright © 2007, Nortel Networks

Event architecture on the Call Server



Event Server

The Event Server receives system events (raw event inputs from system tasks) and processes them. The Event Server then logs the events and sends them to the Event Collector. The Event Server also provides event lookup tables and event processing functions.

There are two tables in the Event Server:

- Event Default Table (EDT)
- Event Preference Table (EPT)

Copyright © 2007, Nortel Networks

EDT

In normal operation, event messages are found in the Event Default Table (EDT). The preconfigured EDT contains the default event severities. Severities from the EDT are assigned to the event severity field of the system messages and traps before the messages are output from the system. The default severities can be overridden by using either EDT Override Mode or the EPT table.

In Small Systems, due to memory constraints, some system messages are omitted from the EDT. In Large Systems, all system messages are included in the EDT.

EDT Override Mode Use LD 117, to set the EDT to operate in a special mode called the *Override Mode*. This mode assigns all events a severity of Minor or Info.

EPT

The Event Preference Table (EPT) is used to store site-specific preferences that override the default severities of the factory-installed EDT. Usually, the EPT is configured by a site administrator and applies to the entire site. The EPT can not be configured for an individual user.

In the EPT, you can perform the following actions:

- override severities assigned in the Event Default Table
- specify severity escalation thresholds
- specify alarm suppression thresholds

Event Collector and System Event List

The Event Collector is the central collection point for events (system messages) that are generated within the system. The Event Collector maintains in memory a list of system events received. The list is called the *System Event List (SEL)*.

One copy of the SEL is saved in memory, and one copy is saved to disk. The disk copy provides data integrity and survivability. The memory-based copy provides quicker access to the data.

System message categories

In CS 1000 and Meridian 1 systems, events, known as *system messages*, are defined by system message categories, such as BUG, ERR, and NWS.

For more information about system messages, see *Software Input/Output System Messages (NN43001-712)*.

Copyright © 2007, Nortel Networks

More information

For more information about the configuration of the Event Server and the Event Collector, see "Event Collector" (page 36) and "Event Server" (page 36).

For more information about overriding severities in the EDT, see "How to change Event Default Table settings" (page 38).

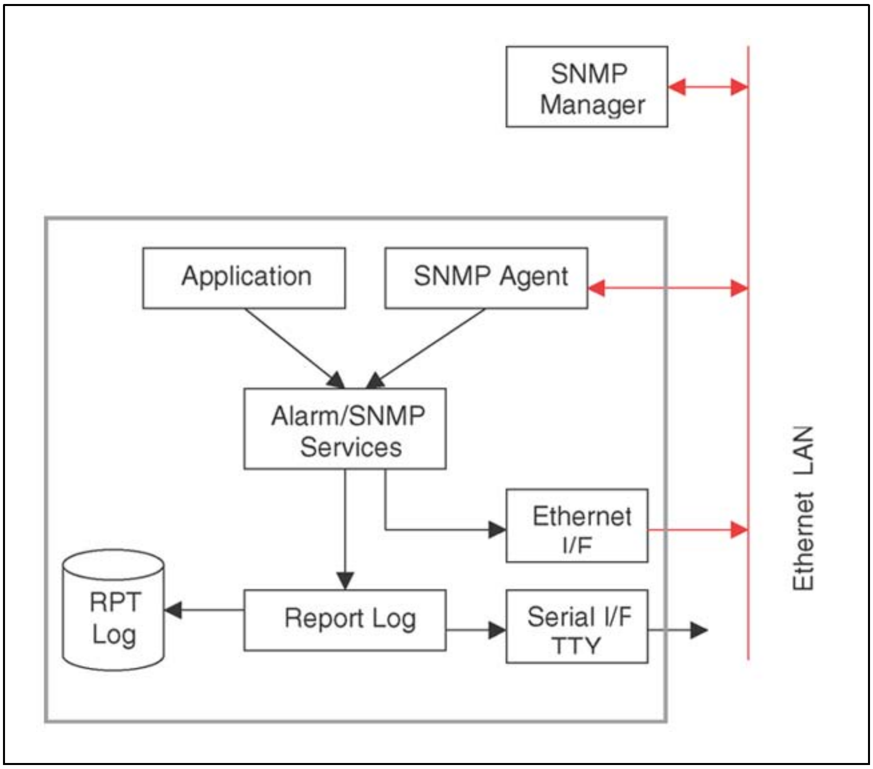
SNMP agent

The SNMP agent receives the SNMPv1 and SNMPv2 queries and takes proper action based on the type of query. The SNMP agent provides access to the standard and Enterprise MIBs defined on the system.

Signaling Server, Voice Gateway Media Card and MGC architecture

The Signaling Server, Voice Gateway Media Card, and MGC architectures are the same and consist of the Alarm/SNMP Services, Report Log, and SNMP agent. See "Event architecture on the Signaling Server, Voice Gateway Media Card, and MGC" (page 24).

Event architecture on the Signaling Server, Voice Gateway Media Card, and MGC



"Trap generation process" (page 25) describes the process of generating an SNMP trap on the Signaling Server, Voice Gateway Media Card, and MGC.

Copyright © 2007, Nortel Networks

Trap generation process

Step	Description
1	The application (for example, IP Line, IP Peer, Gatekeeper, and SIP applications) generates the alarm message.
2	The alarm message is sent to the Alarm Service software that processes the message.
3	The Alarm Service updates the alarm message with the information necessary to generate the alarm as an SNMP trap.
4	The Alarm Service forwards the alarm to the SNMP Agent.
5	The SNMP Agent generates the SNMP trap that is sent out on the ELAN subnet.

Alarm/SNMP Services

The Alarm/SNMP Services is used by the application to raise an alarm and dispatch a trap. The Alarm Services provides the error category and severity of the alarms and sends the alarm to the Report Log for further processing. The SNMP Services converts the alarm into a trap and sends it to the trap destination list. The SNMP Service lets you define a trap destination list. The alarm category and severity can not be configured.

Report Log

The Report Log receives the alarms and takes the proper action to display or log the alarm, based on the required action defined for each error category. You can view the Report Log.

SNMP Agent

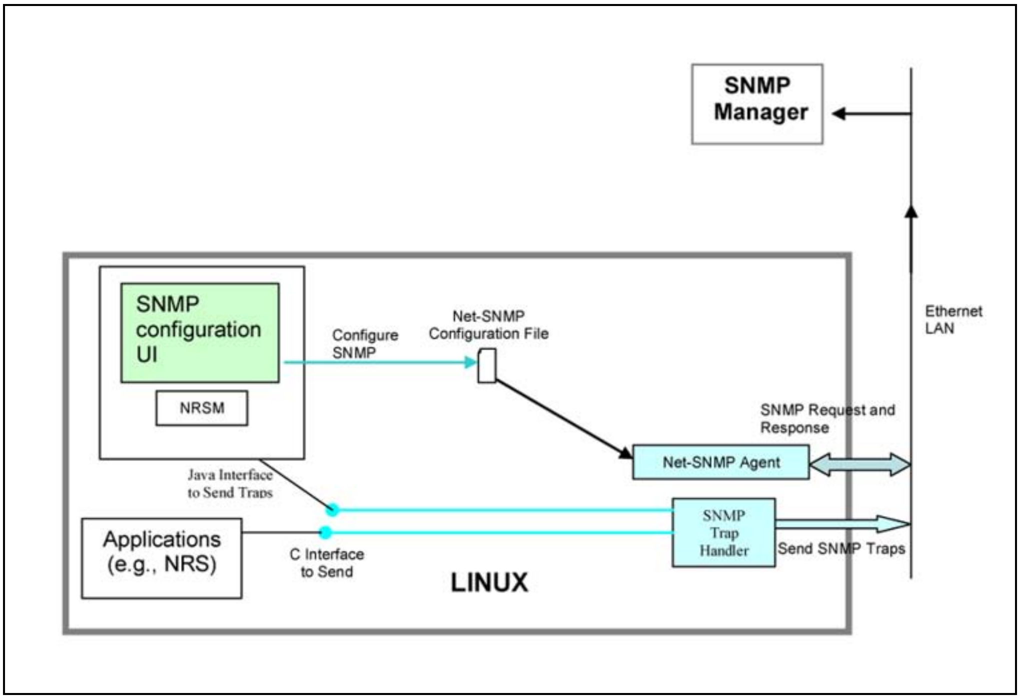
The SNMP Agent receives the SNMP queries and takes the proper action based on the type of query. The SNMP Agent provides access to the standard and Enterprise MIBs defined on the system.

Linux NRS/ECM architecture

The SNMP architecture on Linux is shown in "SNMP architecture on Linux NRS/ECM" (page 26) and is described in the following sections.

Copyright © 2007, Nortel Networks

SNMP architecture on Linux NRS/ECM



Net-SNMP agent

The SNMP capabilities are developed by using the Net-SNMP agent. The agent uses an implementation of the MIB-II objects and responds to SNMP requests.

Configuring SNMP parameters

Configure the SNMP parameters on the Linux server by selecting Tools > SNMP in the navigation pane. Changes are applied to the configuration files used by the Net-SNMP agent and the trap handler components.

Trap Handler component

The Trap Handler component sends SNMP traps in the Common Trap format.

Connections

For more information about connecting the system to the management system, see *Converging the Data Network with VoIP (NN43001-260)*.

Access to SNMP components

The system SNMP interfaces provide alarms from CS 1000 and Meridian 1 systems so that those alarms can be monitored on a Network Management System (NMS).

Copyright © 2007, Nortel Networks

Nortel SNMP capability supports existing NMSs by generating traps to represent system events and alarms. Alarm information is in the traps and includes the following:

- description of the condition that caused the trap to be generated
- severity
- system message identifier (commonMIBErrCode). For information about the system message identifier, see*Software Input/Output System Messages (NN43001-712)*.

For information about trap components, see "Trap format" (page 58).

System SNMP traps can be sent to specified destinations; that is, NMSs or other monitoring systems. Configure a maximum of eight trap destinations for each device.

Network routing table entries

The Call Server has a single ELAN network interface, whereas the Signaling Server, Voice Gateway Media Card, and MGC have both ELAN and TLAN network interface connections. SNMP traps are sent out on the ELAN network interface on all of the devices. When the device sending traps has both ELAN and TLAN network interfaces, the routing table for the device must contain information about the correct network interface (for example, ELAN) and the gateway to be used for each destination.

The associated host route entries for new trap destinations are automatically added to the network routing table for the Signaling Server, Voice Gateway Media Cards, and MGCs.

On Linux systems, the routing table entries are manually added to each NRS or ECM server. To configure the routing table entries on Linux devices, see "Network routing table entries on ECM and Linux NRS" (page 53).

The automatic addition of network routing entries detailed in this section only applies to the routing of configured SNMP traps. It can be necessary to configure network routes to access devices using the ELAN for SNMP MIB queries, or when using other means of access. You can add routing entries to devices using procedures documented in *Element Manager System Administration (NN43001-632)*. The MGC does not have an Element Manager interface to add routing entries. If a routing entry is required on the MGC to any IP address, you can add the IP address as an SNMP trap destination so that the route is automatically added on the MGC. However, a consequence is that SNMP traps from all devices are sent to the specified IP address.

Copyright © 2007, Nortel Networks

Trap and MIB access

"Trap and MIB access" (page 28) lists how device traps and MIBs are accessed.

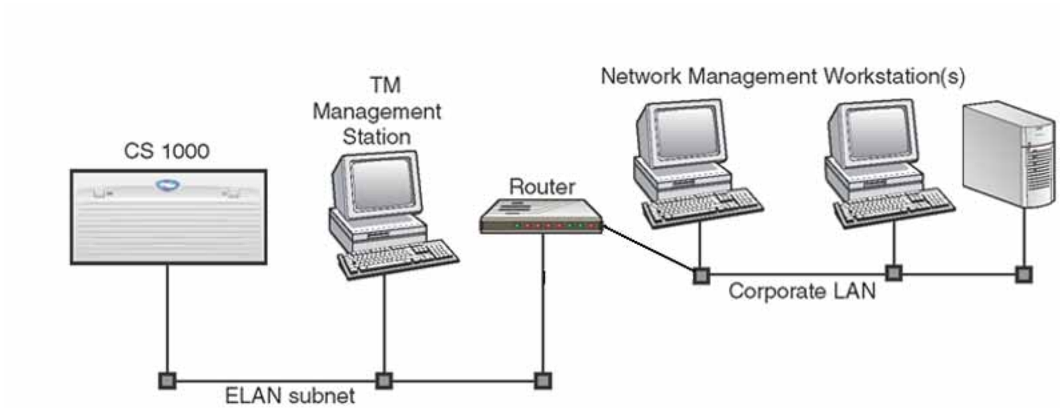
Trap and MIB access

Accessed through the ELAN	Accessed through the TLAN
Call Server traps Signaling Server traps Voice Gateway Media Card traps Media Gateway Controller traps Call Server MIBs Signaling Server MIBs Voice Gateway Media Card MIBs Media Gateway Controller MIBs	Signaling Server Standard MIBs

Sample configuration

One configuration for sending SNMP traps is a dedicated Ethernet configuration using an Ethernet network interface on the system. An example of this configuration is shown in "Typical SNMP Ethernet LAN" (page 28).

Typical SNMP Ethernet LAN



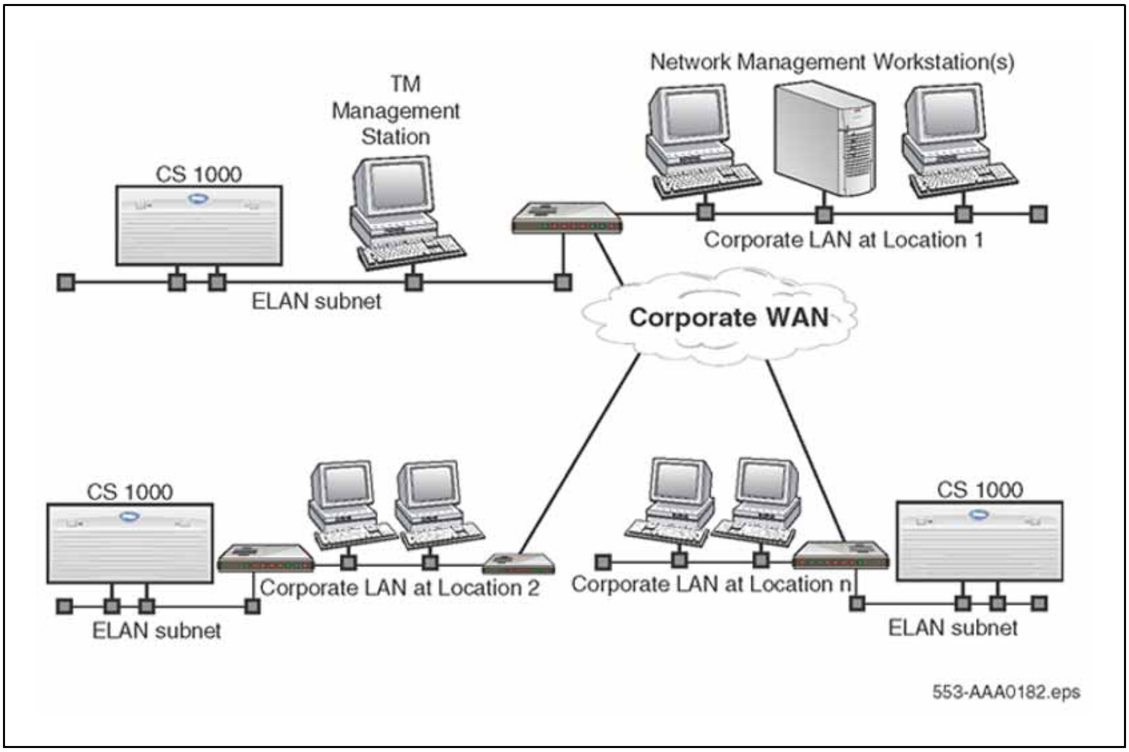
The system Ethernet network interface must reside on a dedicated LAN, the system separated from external LAN traffic. SNMP traps are forwarded through a router or gateway to Network Management workstations residing elsewhere in the network.

Copyright © 2007, Nortel Networks

For a WAN configuration, expand the Ethernet configuration to service multiple systems in or network environments. SNMP traps are forwarded through routers or gateways to Network Management workstation(s) residing somewhere else in the network. This configuration is shown in "Typical SNMP Ethernet WAN" (page 29).

For detailed information about LAN and WAN configuration of Data Networks, see *Converging the Data Network with VoIP (NN43001-260)*.

Typical SNMP Ethernet WAN


Network Management Workstation(s)
TM Management Station
CS 1000
Corporate LAN at Location 1
ELAN subnet
Corporate WAN
CS 1000
CS 1000
Corporate LAN at Location 2
Corporate LAN at Location n
ELAN subnet
ELAN subnet
553-AAA0182.eps

Call Server and IP Telephony device connections

For information about Call Server and IP Telephony device connections, see *Converging the Data Network with VoIP (NN43001-260)*.

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Configuring SNMP

Contents

This chapter contains Information about the following topics:

Overview

You can use various tools (Command Line Interface [CLI], Element Manager, TM, and NRS Manager) to configure SNMP for a system, depending on the system platform (Meridian 1 or CS 1000) and the network device.

SNMP configuration includes the following:

- trap destinations
- community strings (to access MIBs)
- trap community string
- Call Server filtering (EDT, EPT, and alarm suppression thresholds)

"Elements on VxWorks and where they are configured" (page 32) and "Elements on Linux and where they are configured" (page 33) describe where the various elements are configured.

Copyright © 2007, Nortel Networks

Elements on VxWorks and where they are configured

SNMP configuration of	Call Server CLI	Element Manager	Telephony Manager	NRS Manager (VxWorks NRS)
Admin group community strings	Yes See Note 1	Yes See Note 1	Yes See Note 1	Yes See Note 3
Trap community string	Yes See Note 1	Yes See Note 1	No	No
Trap destinations	Yes	Yes	No	Yes
MIB II system group values	Yes	Yes	Yes (Call Server only)	No
EDT/EPT edits	Yes See Note 2	Yes See Note 2	Yes (Call Server only)	No
Alarm suppression threshold edits	Yes See Note 2	Yes See Note 2	No	No

Note 1: The configuration propagates to the Signaling Server, Voice Gateway Media Card, and MGC when the EDD is complete.

Note 2: An EDD must be completed to ensure that the configuration is saved.

Note 3: Support exists only for the system management read/write community strings.

Note: After you configure the community strings on the Call Server, they are synchronized to the Signaling Server, Voice Gateway Media Card, and MGC through a data dump (EDD). Configure the community strings on each Linux element individually since synchronization does not occur on Linux devices.

The NRS on VxWorks resides on a Signaling Server platform. If it coresides with other Signaling Server applications, the SNMP configuration synchronizes with the Call Server. If the VxWorks NRS is a stand-alone application, no other Signaling Server applications run on the same device, and you configure the SNMP parameters by using NRS Manager (NRSM).

The VxWorks NRS supports a subset of the SNMP parameters available on the Call Server. The subset includes the System Management Read and Write community strings and eight trap destinations. Support does not exist for the Admin group community strings, the Trap community string, and other MIB II information. All traps use the public community string.

See "Elements on Linux and where they are configured" (page 33).

Copyright © 2007, Nortel Networks

Elements on Linux and where they are configured

Linux SNMP configuration of	NRS	ECM
Admin group community strings	Yes	Yes
Trap community string	Yes	Yes
Trap destinations	Yes	Yes
MIB II system group values	Yes	Yes

Configuring SNMP on the Call Server using the CLI

The administrator can use the command format in LD 117 to do the following:

- modify the system group parameters for MIB II
- configure or modify the community strings
- configure or modify the Trap community string
- configure or modify the minimum severity level of alarms sent from the Call Server
- configure the Alarm Management features
- propagate community strings to the Signaling Server, Voice Gateway Media Card, and MGC on the system
- send a test alarm
- create, modify, and delete EPT entries
- import, export, and reload the EPT file
- print the EDT and EPT entries
- print an event list sorted by severity

Both administration and maintenance commands appear in LD 117.

Command format

LD 117 uses a Command Line input interface (input parser) that has the following general structure (where => is the command prompt):

```
=> COMMAND OBJECT[(FIELD1 value) (FIELD2 value)...  (FIELDx
value)]
```

LD 117 provides the following configuration features:

- **Context Sensitive Help**

  Help is offered when **?** is entered. The Help context is determined by the position of the **?** entry in the command line. If **?** is entered in the COMMAND position, Help text is displayed that presents all applicable command options. If **?** is entered in the OBJECT position, HELP text is displayed that presents all applicable OBJECT options.

Copyright © 2007, Nortel Networks

- **Abbreviated Inputs**

  The input parser recognizes abbreviated inputs for commands, objects, and object fields. For example, `N` can be entered for the command NEW, or `R` can be entered for the object Route.

- **Optional Fields**

  Object fields with default values can be bypassed by the user on the command line. For example, to configure an object that consists of fields with default values, enter the command, the object name, and press **<enter>**. You do not have to specify all object fields.

> **ATTENTION**
>
> Nortel recommends that you perform a data dump after SNMP configuration to retain the changes. A data dump must be performed if any changes are made to the SNMP parameters.

Configuring target IP address

On a Call Server, use the LD 117 command `SET OPEN_ALARM` to configure the target IP addresses of the SNMP Manager.

Use LD 117 commands to configure the SNMP Agent to send out SNMP traps to the IP address of the management system. Specify up to eight SNMP trap destinations (IP addresses) for the Call Server, Signaling Servers, Voice Gateway Media Cards, and MGCs.

For the command syntax, see "Commands - alphabetical order" (page 41).

Verifying the SNMP configuration

When the SNMP installation and setup is complete, verify that the configuration is operational. To verify the configuration, follow the steps in "Verifying the SNMP configuration" (page 34).

Verifying the SNMP configuration

Step Action

1 Verify the system Ethernet connection. Use the standard PING command to ping the switch for a response. If there is no response, verify the Ethernet hardware, cabling, and configuration.

2 Verify that the system SNMP Agent is alive. The following MIB II variables are queried by using a standard MIB browser, available on the NMS:

- SysUpTime
- SysDescr

Copyright © 2007, Nortel Networks

- SysObjectId.

3 Verify that SNMP traps are sent and received correctly. In LD 117, use the `TEST ALARM` command to manually generate a trap that is sent to each alarm destination IP address configured on the Call Server.

—End—

TEST ALARM command

Use a diagnostic utility for alarm testing by entering a command in LD 117. The Test Alarm utility simulates an alarm to verify that the alarms are generated correctly and are sent to their configured destinations. The alarm is sent to the trap destination list configured on the system by using LD 117.

The `TEST ALARM` command creates and sends an SNMP trap to the trap destination list, and a message appears on the console. The alarm test utility sends a trap for any specified parameter.

The flow of the message goes through the following:

- Event Default Table (EDT) to assign the correct severity if the system message is valid; otherwise, the system message is assigned a severity of Info.
- Event Preference Table (EPT) to modify the severity or suppress the system message, based on a threshold.

The system message is sent to the TTY, is written to the System Event List (SEL), and is sent as a trap. The severity of the trap follows the severity of the existing message that is defined by the EDT and EPT. A nonexistent system message has a severity of Info.

If the Test Alarm utility uses a valid system message and sends a trap to the trap destination correctly, it does not guarantee that the same system message, if it occurs, is sent as a trap. Some system messages, such as SCH, do not generate a corresponding trap, but provide operator feedback.

See "Commands - alphabetical order" (page 41) for the TEST ALARM command syntax.

Overview of Alarm Management on the Call Server

With the Alarm Management feature, all processor-based system events are processed and logged into a disk-based SEL.

Copyright © 2007, Nortel Networks

Events such as BUG and ERR error messages, that are generated as a result of maintenance or system activities, are logged into the SEL. Events generated as a result of administration activities, such as SCH or ESN error messages, are not logged into the SEL. Unlike the System History File, this System Event List survives Sysload, Initialization, and power failures.

Event Collector

The Event Collector captures and maintains a list of all processor-based system events on the Call Server. The Event Collector also routes critical events to TTY ports and lights the attendant console minor alarm lamp as appropriate. You can print or browse the SEL.

Event Server

The Event Server consists of two components:

1. **Event Default Table (EDT)**: This table associates events with a default severity. By using the `CHG EDT` command in LD 117, the EDT is overridden so that all events are set to the configured severity. You can also view the EDT with the commands in LD 117. The EDT is stored in a disk file but is scanned into memory on startup for rapid run-time access. "Sample Event Default Table entries" (page 36) lists examples of Event defaults.

   Sample Event Default Table entries

Error Code	Severity
ERR220	Critical
IOD6	Critical
BUG4001	Minor

   > ***Note:*** Error codes that do not appear in the EDT are assigned a default severity of Info.

2. **Event Preference Table (EPT)**: This table contains site-specific preferences for event severities as well as criteria for severity escalation and alarm suppression. The administrator configures the EPT to do the following:

   a. override the default event severity assigned by the default table

   b. escalate the event severity of frequently occurring minor or major alarms

See an example of an EPT in "Sample Event Preference Table (EPT)" (page 37).

Copyright © 2007, Nortel Networks

Sample Event Preference Table (EPT)

Error Code	Severity	Escalate Threshold (events/60 sec.) (see Note 2)
INI???	Default	7
ERR??? (see Note 1)	Critical	5
BUG1??	Minor	0
HWI363	Major	3

Note 1: The question mark (?) is a wildcard. See "Wildcards" (page 37) for an explanation of wildcard entries.

Note 2: The window timer length defaults to 60 seconds, however, the administrator can change this value. See "Global window timer length" (page 38) for more information.

After the alarm goes through the EDT and the EPT, the severity level is checked against the alarm suppression threshold. The **`CHG SUPPRESS_ALARM`** command is used to configure the minimum severity of alarms that are sent from the system.

Wildcards

The special wildcard character **?** can be entered for the numeric segment of an error code entry in the EPT to represent a range of events. All events in the range indicated by the wildcard entry can then be assigned a particular severity or escalation threshold.

For example, if **ERR? ???** is entered and assigned a MAJOR severity in the EPT, all events from ERR1000 to ERR9999 are assigned MAJOR severity. If **BUG3?** is entered and assigned an escalation threshold of five, the severity of all events from BUG0030 to BUG0039 is escalated to the next higher severity if their occurrence rate exceeds five per time window.

The wildcard character format is as follows:

- **`ERR?`** = ERR0000 - ERR0009
- **`ERR??`** = ERR0010 - ERR099
- **`ERR???`** = ERR0100 - ERR0999
- **`ERR????`** = ERR1000 - ERR9999

Escalation and suppression thresholds

The escalation threshold specifies a number of events per window timer length that, when exceeded, causes the event severity to be escalated up one level. The window timer length is set to one minute by default. Escalation occurs only for minor or major alarms. Escalation threshold values must be less than the universal suppression threshold value.

Copyright © 2007, Nortel Networks

A suppression threshold suppresses events that flood the system, and applies to all events. It is set to 15 events per minute by default.

Global window timer length Both the escalation and suppression thresholds are measured within a global window timer length. The window timer length is set to one minute by default. However, you can change the window timer length by using the **`CHG TIMER`** command in LD 117. See "Commands - alphabetical order" (page 41).

EDT/EPT configuration

Commands are available in LD 117 to configure the parameters of the EDT and EPT.

The commands use the following general structure, where => is the command prompt, commands and objects are in bold type, and fields are in regular type. Fields enclosed in parenthesis ( ) are default values.

How to change Event Default Table settings

The EDT contains the default severities for the alarms in the system. You can change some of the default severities by using the EPT or by using commands that reset all alarms in the EDT to either Info or Minor severity. Use the LD 117 **`CHG EDT`** command to configure all of the event severities in the EDT to Minor or Info.

Minor The command to change default severities to Minor is

```
CHG EDT Minor
```

The severity of all events in the EDT is configured as Minor.

Info The command to change default severities to Info is

```
CHG EDT Info
```

The severity of all events in the EDT is configured as Info.

Changing Event Preference Tables

You can configure the individual event severities in the Event Preference Table (EPT) to Info, Minor, Major, or Critical. You can also set a different escalation suppression value for a specific message by using the EPT.

The escalation threshold value must be less than the Global Suppression threshold value. The Global Suppression threshold value is defined as the number of occurrences of an event within the global timer window.

Use the **`PRT SUPPRESS`** command to find the Global Suppression threshold value.

Copyright © 2007, Nortel Networks

Use the **`PRT SUPPRESS_ALARM`** command to find the alarm severity threshold value.

Use the **`CHG EPT`** command to change the severities in the EPT:

```
  CHG EPT <EPT entry> [<SEVERITY> <ESCALATE>]
```

Wildcard characters Use wildcard characters for entries in the EPT. See "Wildcards" (page 37) for more information.

Community strings

Read-only and read/write community strings control access to all MIB data. Support exists for a set of administrator community strings with read-only privileges with the default strings of admingroup1, admingroup2, and admingroup3.

Use commands in LD 117 to configure MIB community strings for access to Call Server MIBs (MIB-II objects), Signaling Server, Voice Gateway Media Card, and MGC MIBs. "Call Server default community strings" (page 39) lists the Call Server community strings. "Signaling Server, Voice Gateway Media Card, and MGC default community strings" (page 40) lists the Signaling Server, Voice Gateway Media Card, and MGC community strings.

Call Server default community strings

Community Name (User group)	Access privileges	Interface	View
admingroup1 **`[ADMIN_COMM(1)]`**	read	ELAN	MIB II
admingroup2 **`[ADMIN_COMM(2)]`**	read	ELAN	MIB II Nortel Management Proprietary MIB
admingroup3 **`[ADMIN_COMM(3)]`**	read	ELAN	MIB II
public **`[SYSMGMT_TRAP_COMM]`**	No access See Note	See Note	No access See Note
otm123 **`[SYSMGMT_RD_COMM]`**	read	ELAN	MIB II
otm321 **`[SYSMGMT_WR_COMM]`**	read/write	ELAN	Nortel Management Proprietary MIB

Note: Used only in SNMP traps and provides no access to the MIBs.

Copyright © 2007, Nortel Networks

Signaling Server, Voice Gateway Media Card, and MGC default community strings

Community Name (User group)	**Access privileges**	**Interface**	**View**
admingroup1 `[ADMIN_COMM(1)]`	read	ELAN	MIB II
admingroup2 `[ADMIN_COMM(2)]`	read	ELAN	MIB II QOS-MIB.mib (also known as Zonetrafficrpt MIB - Signaling Server only) Nortel Management Proprietary MIB
admingroup3 `[ADMIN_COMM(3)]`	read	ELAN	MIB II QOS-MIB.mib (also known as Zonetrafficrpt MIB - Signaling Server only) Nortel Management Proprietary MIB
public `[SYSMGMT_TRAP_COMM]`	No access See Note	See Note	No access See Note
otm123 `[SYSMGMT_RD_COMM]`	read	ELAN	MIB II QOS-MIB.mib (also known as Zonetrafficrpt MIB - Signaling Server only) Nortel Management Proprietary MIB
otm321 `[SYSMGMT_WR_COMM]`	read/write	ELAN	MIB II QOS-MIB.mib (also known as Zonetrafficrpt MIB - Signaling Server only) Nortel Management Proprietary MIB
Note: Used only in SNMP traps and provides no access to the MIBs.			

Linux NRS and ECM community strings

Community name (User group)	**Access privileges**	**Interface**	**View**
admingroup1 `[ADMIN_COMM(1)]`	read	ELAN	MIB II
admingroup2 `[ADMIN_COMM(2)]`	read	ELAN	MIB II

Copyright © 2007, Nortel Networks

Community name (User group)	**Access privileges**	**Interface**	**View**
admingroup3 `[ADMIN_COMM(3)]`	read	ELAN	MIB II
public `[SYSMGMT_TRAP_COMM]`	No access See Note	See Note	No access See Note
otm123 `[SYSMGMT_RD_COMM]`	read	ELAN	MIB II
otm321 `[SYSMGMT_WR_COMM]`	read	ELAN	MIB II
Note: Used only in SNMP traps and provides no access to the MIBs.			

The following commands are used to configure and print the community strings:

- **`CHG ADMIN_COMM`**
- **`CHG SYSMGMT_TRAP_COMM`**
- **`CHG SYSMGMT_RD_COMM`**
- **`CHG SYSMGMT_WR_COMM`**
- **`PRT ADMIN_COMM`**
- **`PRT SYSMGMT_COMM`**

See "Commands - alphabetical order" (page 41) for the command syntax.

The community strings used by the Signaling Server, Voice Gateway Media Card, and MGC are configured on the Call Server and synchronized to these elements when a data dump is performed. As well, the community strings are synchronized when a link is established between any of these elements and the Call Server.

> ***Note:*** The synchronization of community strings does not occur between the Linux NRS and ECM and the Call Server. You must separately configure each Linux NRS and ECM device.

SNMP CLI commands

Commands - alphabetical order

=> Command	**Description**
`CHG ADMIN_COMM n aa...a`	Changes the admin groups community string, where: • **`n`** = a number from one to three • **`aa...a`** = a string with a maximum length of thirty-two characters

Copyright © 2007, Nortel Networks

=> Command	Description
	Default(1) = admingroup1* Default(2) = admingroup2 * Default(3) = admingroup3 * These communities are used to access different SNMP objects on the Call Server, Signaling Servers, Voice Gateway Media Card, and MGC. * – case-sensitive
`CHG EDT INFO`	Overrides the EDT; use INFO as the default severity for all events except those specified in the Event Preference Table (EPT).
`CHG EDT MINOR`	Overrides the EDT; use MINOR as the default severity for all events except those specified in the Event Preference Table (EPT).
`CHG EDT NORMAL`	Uses the Event Default Table (EDT) default severities.
`CHG EPT aa... a CRITICAL x`	Changes an EPT entry to Critical severity, where: • `aa... a` = an event class with an event number (for example, BUG1000, ERR0025) • `x` = optional entry to escalate the value of the EPT entry from (0)-Suppress value, as defined by the default or the`CHG SUPPRESS` entry
`CHG EPT aa... a EDT x`	Changes the EPT to an NT-defined severity from the EDT, where: • `aa... a` = an event class with an event number (for example, BUG1000, ERR0025) • `x` = optional entry to escalate the value of the EPT entry from (0)-Suppress value, as defined by the default or the`CHG SUPPRESS` entry
`CHG EPT aa... a INFO x`	Changes an Event Preference Table (EPT) entry to Information severity, where: • `aa... a` = an event class with an event number (for example, BUG1000, ERR0025) • `x` = optional entry to escalate the value of the EPT entry from (0)-Suppress value, as defined by the default or the`CHG SUPPRESS` entry
`CHG EPT aa... a MAJOR x`	Changes an EPT entry to Major severity, where:

Copyright © 2007, Nortel Networks

=> Command	Description
	- **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) - **x** = optional entry to escalate the value of the EPT entry from (0)-Suppress value, as defined by the default or the**CHG SUPPRESS** entry
`CHG EPT aa... a MINOR x`	Changes an EPT entry to Minor severity, where: - **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) - **x** = optional entry to escalate the value of the EPT entry from (0)-Suppress value, as defined by the default or the**CHG SUPPRESS** entry
`CHG SELSIZE 5-(500)-2000`	Changes the System Event List Size (the number of events in the SEL).
`CHG SNMP_SYSCONTACT aa... a`	Change the contact person name for this system element (machine). Where aa...a = a string with a maximum length of 100 characters. Default = System Contact. ***Note:*** Use a single X to clear the field.
`CHG SNMP_SYSLOC aa...a`	Change the defined physical location for this system element (machine). Where aa...a = a string with a maximum length of 100 characters. Default = System Location. ***Note:*** Use a single X to clear the field.
`CHG SNMP_SYSNAME aa...a`	Change the system name assigned to this system element (machine). Where aa...a = a system name string with a maximum length of 100 characters. - can include a %hostname% variable that will be substituted with the physical hostname of a system element. Default SNMP System Name = "System Name". ***Note:*** Use a single X to clear the field.
`CHG SUPPRESS 5-(15)-127`	Changes the global suppression for events (the number of occurrences within the global timer window before the event is suppressed).

Copyright © 2007, Nortel Networks

=> Command	Description
CHG SUPPRESS_ALARM n	Changes the minimum alarm severity threshold of the alarms that are sent, where **n** is: - 0 = All - 1 = Minor - 2 = Major - 3 = Critical
CHG SYSMGMT_RD_COMM aa...a	Changes the system management read-only community string where: **aa...a** = a string with a maximum length of thirty-two characters
CHG SYSMGMT_TRAP_COMM aa...a	Changes the Trap community string where: **aa...a** = a string with a maximum length of thirty-two characters
CHG SYSMGMT_WR_COMM aa...a	Changes the system management read/write community string where: **aa...a** = a string with a maximum length of thirty-two characters
CHG TIMER (1)-60	Changes the global timer window length in minutes. See "Global window timer length" (page 38).
NEW EPT aa... a CRITICAL x	Assigns a Critical severity to a new EPT entry, where: - **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) - **x** = optional entry to escalate the value of the EPT entry from (0)–Suppress value, as defined by the default or the**CHG SUPPRESS** entry
NEW EPT aa... a EDT x	Assigns an NT-defined severity from the EDT to a new EPT entry, where: - **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) - **x** = optional entry to escalate the value of the EPT entry from (0)–Suppress value, as defined by the default or the**CHG SUPPRESS** entry
NEW EPT aa... a INFO x	Assigns an Information severity to a new EPT entry, where:

Copyright © 2007, Nortel Networks

=> Command	Description
	• **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) • **x** = optional entry to escalate the value of the EPT entry from (0)–Suppress value, as defined by the default or the**CHG SUPPRESS** entry
NEW EPT aa... a MAJOR x	Assigns a Major severity to a new EPT entry, where: • **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) • **x** = optional entry to escalate the value of the EPT entry from (0)–Suppress value, as defined by the default or the**CHG SUPPRESS** entry
NEW EPT aa... a MINOR x	Assigns a Minor severity to a new EPT entry, where: • **aa... a** = an event class with an event number (for example, BUG1000, ERR0025) • **x** = optional entry to escalate value of EPT entry from (0)–Suppress value, as defined by default or the**CHG SUPPRESS** entry
OUT EPT aa... a	Deletes a single Event Preference Table (EPT) event, where: • **aa... a** = an event class with an event number (for example, BUG1000, ERR0025)
OUT EPT ALL	Deletes all of the entries in Event Preference Table (EPT).
PRT ADMIN_COMM	Prints the administration group read-only community strings.
PRT EDT aa... a	Prints a single Event Default Table (EDT) event, where: • **aa... a** = an event class with an event number (for example, BUG1000, ERR0025)
PRT EDT aa... a bb...b	Prints a range of Event Default Table (EDT) events, where: • **aa... a** = first entry in EDT event range (for example, BUG1000, ERR0025) • **bb...b** = last entry in the EDT event range (for example, BUG1000, ERR0025)
PRT EPT aa... a	Prints a single Event Preference Table (EPT) entry, where: • **aa... a** = an event class with an event number (for example, BUG1000, ERR0025)
PRT EPT aa... a bb...b	Prints a specific Event Preference Table (EPT) entry, where:

Copyright © 2007, Nortel Networks

=> Command	Description
	• `aa... a` = first entry in the EPT event range (for example, BUG1000, ERR0025) • `bb...b` = last entry in the EPT event range (for example, BUG1000, ERR0025)
`PRT EPT ALL`	Prints all of the entries in Event Preference Table (EPT)
`PRT OPEN_ALARM`	Prints the settings for all open SNMP traps (alarms). Only active slots are displayed.
`PRT SEL nn`	Prints the most recent records in the system event list, where: `nn` = 0-(20)-SELSIZE. For example, if `nn` = 50, the 50 most recent events in the system event list are printed.
`PRT SELSIZE`	Prints the System Event List size.
`PRT SUPPRESS`	Prints the global suppress value.
`PRT SUPPRESS_ALARM`	Prints the alarm suppression threshold value.
`PRT SYSMGMT_COMM`	Prints the system management community strings and Trap community strings.
`PRT TIMER`	Prints the global timer window length (in minutes). See "Global window timer length" (page 38).
`SET OPEN_ALARM <slot> <IP address>`	Adds an SNMP trap destination (Network Management System). • `Slot value` = 0 to 7 • The address format is: x.x.x.x. (TCP/IP) `x>` = 0 `x` = 255
`SET OPEN_ALARM <slot> 0.0.0.0`	Removes an SNMP trap destination. `Slot value` = 0 to 7
`TEST ALARM aaaa nnnn`	Generates an alarm, where: • `aaaa` = any character sequence. However, to test how an existing system message category (for example, BUG, ERR, INI) appears in an alarm browser, use an existing system message. • `nnnnn` = any numeric sequence (for example, 1234, 3458) and is optional, defaulting to 0000 The actual output on the TTY is the system message used as the parameter. For example:

Copyright © 2007, Nortel Networks

=> Command	Description
	BUG1234 The actual trap sent to the trap destination list has the same severity of an existing message, which is defined by the EDT and EPT. Nonexistent system messages have a severity of **Info**. The following items are found in the details section of the trap output: **commonMIBDateAndTime:** = the time when the test is generated **commonMIBSeverity:** = defined by the EDT and EPT or **Info(5)** **commonMIBComponentID:** = the configured value of the Navigation system name: Navigation site name: CS (component type) **commonMIBNotificationID:** = 0 **commonMIBSourceIPAddress:** = <IP Address of Call Server> **commonMIBErrCode:** = <AAAANNNN> **commonMIBAlarmType:** = 8 (indicating unknown) **commonMIBProbableCause:** = 202 (indicating unknown) **commonMIBAlarmData:** = Contains textual description The rest of the variable bindings are NULL.

SNMP configuration using Element Manager

This section describes how to use Element Manager to configure SNMP on the Call Server, Signaling Server, and IP Telephony devices. After you configure the SNMP parameters on the Call Server, the configuration synchronizes with the Signaling Server, Voice Gateway Media Cards, and MGCs. Use Element Manager to configure SNMP trap destinations and community strings for CS 1000 systems.

For information about community strings, see "Community strings" (page 39).

Configuring SNMP on the Call Server

Follow the steps in "Configuring SNMP on the Call Server" (page 48) to configure SNMP on the Call Server.

Copyright © 2007, Nortel Networks

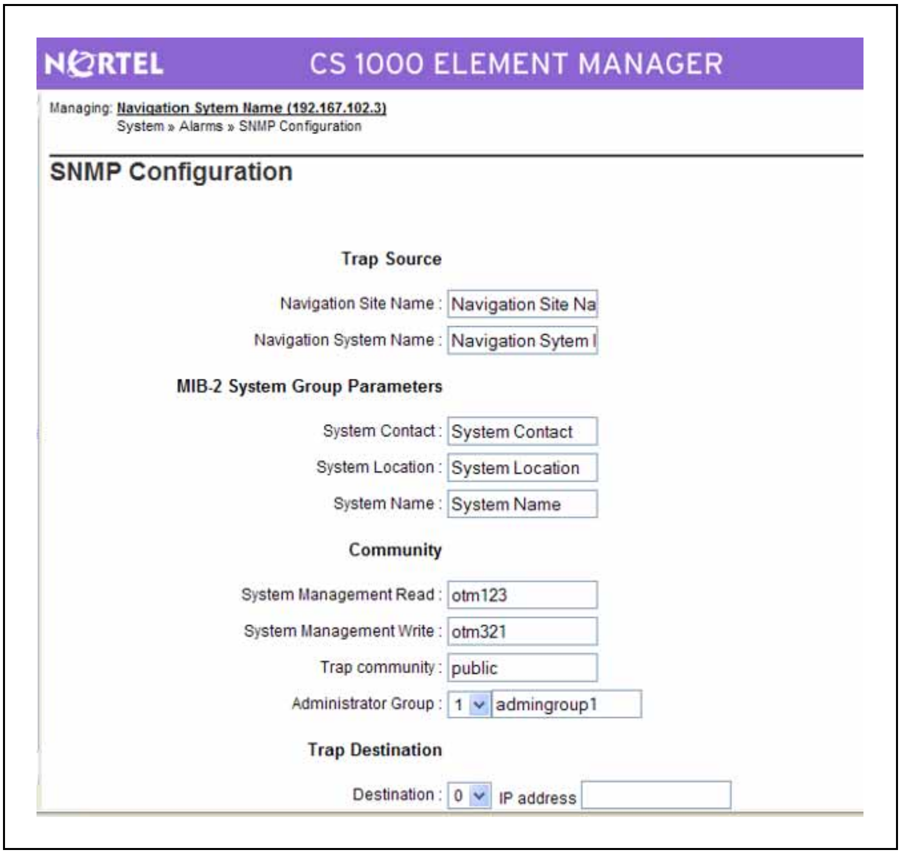
Configuring SNMP on the Call Server

Step Action

1 In the Element Manager navigator pane, choose **System > Alarms > SNMP**.

The SNMP Configuration window appears. See "SNMP Configuration window" (page 48).

SNMP Configuration window



Managing: Navigation Sytem Name (192.167.102.3)
System » Alarms » SNMP Configuration

SNMP Configuration

Trap Source

Navigation Site Name : Navigation Site Na
Navigation System Name : Navigation Sytem I

MIB-2 System Group Parameters

System Contact : System Contact
System Location : System Location
System Name : System Name

Community

System Management Read : otm123
System Management Write : otm321
Trap community : public
Administrator Group : 1 adminogroup1

Trap Destination

Destination : 0 IP address

2 Obtain the following information from the system administrator and enter it in the appropriate fields.

- Navigation Site Name (NAV_SITE)
- Navigation System Name (NAV_SYSTEM)
- Contact Person for this machine (SNMP_SYSCONTACT)
- Physical Location of this machine (SNMP_SYSLOC)
- Name assigned to this machine by the administrator (%hostname%)

Copyright © 2007, Nortel Networks

- System Management Read community string (SYS-MGMT_RD_COMM)
- System Management Write community string (SYS-MGMT_WR_COMM)
- System Management Trap community string (SYS-MGMT_TRAP_COMM)
- Admin Group community string (ADMIN_COMM). Select 1, 2, or 3 from the drop-down list.
- SNMP trap destination address – see step 3

Note: All community strings, except the Trap community string, must be unique. They cannot be the same.

3 In the **SNMP trap destination address** field, enter the IP address of the trap destinations.

SNMP traps are sent to the IP addresses that are entered here.

If applicable, add destination SNMP Manager IP addresses for the following:

- local TM server
- Point to Point Protocol (PPP) IP address configured in the router on the ELAN subnet for the TM PC
- SNMP manager for alarm monitoring

You can enter a maximum of eight trap destinations. They are numbered from zero to seven. Select the trap destination number from the drop-down list.

Note: To remove a trap destination from the trap destination list, select the number from the list and delete the IP address from the IP address field.

4 Click **Save** to save and synchronize the configuration or click **Cancel** to cancel the entry.

5 Perform a data dump to permanently save and synchronize the community strings to Signaling Server, Voice Gateway Media Card, and MGC.

Note: See LD 117 in the *Software Input/Output Administration (NN43001-611)*.

—End—

Copyright © 2007, Nortel Networks

Configuring SNMP using stand-alone NRS

The NRS (on Vxworks, stand-alone mode only) generates SNMP traps and sends them to a configured SNMP host. The NRS uses the SNMP services provided by the Signaling Server platform.

The SNMP settings in NRS Manager (NRSM) are available only when the connected NRS is in stand-alone mode. If the connected NRS is in coresident mode, the SNMP Settings section is not displayed in NRS Manager. Instead, the SNMP parameters are configured by using Element Manager.

Configuration of SNMP parameters on stand-alone NRS include system management community strings, trap destinations, and the enabling or disabling of the trap destination flag.

Configure SNMP on NRS

Step	Action
1	Log on to NRS Manager with a valid user account.
2	On the **Home** tab, choose **System Wide Settings > NRS Server Settings** to configure the **SNMP Settings**.
3	In **Read community name**, enter a community string.
4	In **Write community name**, enter a community string.
5	Select **SNMP traps enabled**.
6	In **Trap destination IP 1**, enter the IP address for the destination to which the trap is sent. Add up to eight trap destinations, if required.
7	Click **Save**. The configured settings are saved and require a system restart to take effect. The new values are updated after the system is restarted.

—End—

Configuring SNMP on ECM and Linux NRS

To configure the SNMP parameters with ECM and Linux NRS, follow the steps in "Configuring SNMP using ECM" (page 51). Configure the SNMP parameters on each device if more than one ECM or Linux NRS server exists on the network.

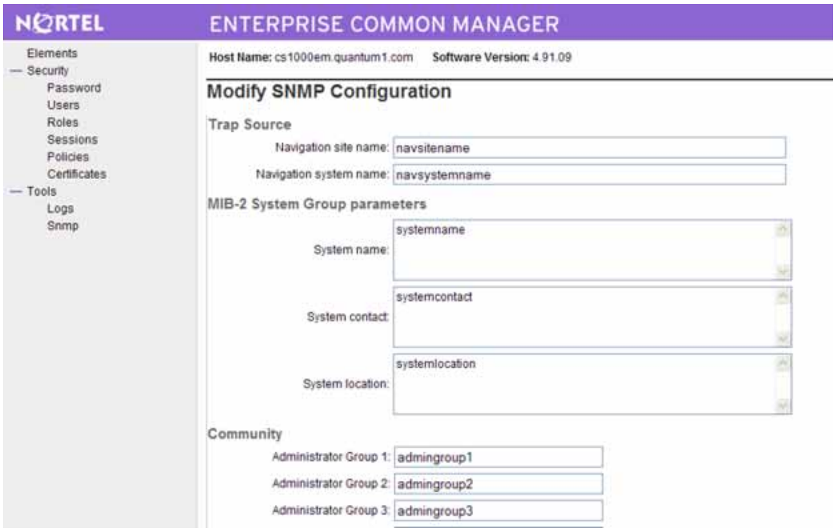
Copyright © 2007, Nortel Networks

Configuring SNMP using ECM

Step	Action
1	In a Web browser, type the IP address of the Linux device. For example, **https://<IP address>**. ***Note:*** You can use the Fully Qualified Domain Name (FQDN) of the Linux device to log on, for example, **https://cs1000ecm.quantum3.com**.
2	Log on with a valid user account.
3	In the Navigator pane, choose **Tools > SNMP**. The SNMP Configuration window appears.
4	Click **Edit**. The Modify SNMP Configuration window appears. See "Modify SNMP Configuration on ECM (a)" (page 52).
5	Obtain the following information from the system administrator and enter it in the appropriate fields. • Navigation Site Name • Navigation System Name • Contact Person for this machine • Physical Location of this machine • Admin Group community string. Select 1, 2, or 3 from the list. • System Management Read community string • System Management Write community string • SNMP Trap community string • SNMP trap destination address (see step 6) ***Note:*** All community strings, except the Trap community string, must be unique. They cannot be the same.

Copyright © 2007, Nortel Networks

Modify SNMP Configuration on ECM (a)



Host Name: cs1000em.quantum1.com **Software Version:** 4.91.09

Modify SNMP Configuration

Trap Source

Navigation site name: navsitename

Navigation system name: navsystemname

MIB-2 System Group parameters

System name: systemname

System contact: systemcontact

System location: systemlocation

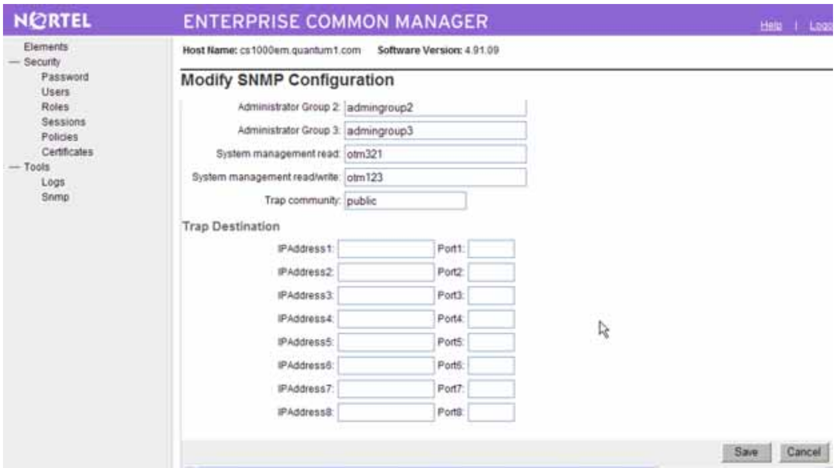
Community

Administrator Group 1: admingroup1

Administrator Group 2: admingroup2

Administrator Group 3: admingroup3

Modify SNMP configuration on ECM (b)



Host Name: cs1000em.quantum1.com **Software Version:** 4.91.09

Modify SNMP Configuration

Administrator Group 2: admingroup2

Administrator Group 3: admingroup3

System management read: otm321

System management read/write: otm123

Trap community: public

Trap Destination

IPAddress1: Port1:

IPAddress2: Port2:

IPAddress3: Port3:

IPAddress4: Port4:

IPAddress5: Port5:

IPAddress6: Port6:

IPAddress7: Port7:

IPAddress8: Port8:

6 Scroll down to configure the SNMP trap destinations.

In the **Trap Destination** section, enter the IP addresses of the trap destinations and the corresponding port numbers, shown in "Modify SNMP configuration on ECM (b)" (page 52).

> ***Note:*** The default port number for SNMP traps is 162.

SNMP traps are sent to the IP addresses that are entered here.

Copyright © 2007, Nortel Networks

Add destination SNMP Manager IP addresses for the following, if applicable:

- local TM server
- PPP IP address configured in the router on the ELAN subnet for the TM PC
- SNMP manager for alarm monitoring.

You can enter a maximum of eight trap destinations numbered from one to eight.

> ***Note:*** Remove a trap destination from the trap destination list, by deleting the IP address and port number in the appropriate fields.

7 Click **Save** to save the configuration or **Cancel** to cancel the entry.

—End—

Network routing table entries on ECM and Linux NRS

Configure SNMP trap destination IP addresses in the network routing table on each ECM and Linux NRS server.

SNMP traps are usually routed through the ELAN network interface. However, ECM and Linux NRS servers can also have a TLAN network interface. Therefore, the configuration must include the correct interface and gateway.

Repeat the configuration on each server since synchronization does not occur between Linux servers.

The routing table entries that are created in "Configuring network routing table entries on ECM and Linux NRS" (page 54) are retained if the server is rebooted.

Copyright © 2007, Nortel Networks

Configuring network routing table entries on ECM and Linux NRS

Step	Action
1	Log on to the Linux CLI using the root user account. At the prompt, create a system-routing file for the ELAN network interface (eth0).
2	Type **`vi /etc/sysconfig/network-scripts/route-eth0`**.
3	Press **`enter`**. The *route-eth0* system routing file appears.
4	Enter Insert mode on the system, type **`i`**. ***Note:*** In the vi editor, Normal mode is the default mode after you log on. In Normal mode you can only enter commands. To enter text, switch to Insert mode, as in step 4 of this procedure.
5	Add a host routing entry for each SNMP trap destination, type **`<IP address>/32 via <gateway>`**. Where: • <IP address> = the SNMP trap destination IP address • <gateway> = the gateway on the ELAN subnet used to reach this destination. **Example:** `192.168.205.15/32 via 192.168.55.1`
6	Press **`enter`**. Repeat step 5 for each host routing entry to a maximum of eight entries.
7	Exit Insert mode, press **`esc`**. The vi editor is in Normal mode.
8	Refresh the routing table and the host route entries appear.
9	Type **`/etc/sysconfig/network-scripts/ifup-routes eth0`**.
10	Save and close the file, by pressing the following key sequence:**`:wq`**. The routing table entries are added and parsed when the server reboots. Use the command line in step 2 to add, modify, or delete SNMP trap destination IP addresses in the routing table on each server.

Copyright © 2007, Nortel Networks

In Normal mode, type **x** to delete the character above the cursor.

Use the **route -n** command to list the configured routes after they are saved.

> ***Note:*** You cannot save changes to the file by using the **:q!** command. To save and close the file, see step 9 in this procedure.

To exit the *route-eth0* system routing file without saving, press the following key sequence: **:q!**

—End—

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Traps

Contents

This chapter contains information about the following topics:

Overview

In general, a Meridian 1 or CS 1000 SNMP trap contains the following data:

- ELAN IP address of the node from which the trap is generated
- error code (system message identifier)
- description of the condition that caused the trap to be generated
- severity
- component name
- event time
- event type

Trap MIBs

A Common Trap MIB (**COMMON-TRAP-MIB.mib**) with new trap OIDs is defined, to provide a common format for all elements.

Copyright © 2007, Nortel Networks

For more information, see "MIBs" (page 63).

Standard traps

In addition to the Nortel traps that are sent using the Common Trap format, other traps are sent by CS 1000 elements, such as coldStart, warmStart, and other standard traps defined by RFC 1157. Linux devices send traps from the Net-SNMP agent, as defined in the NET-SNMP-AGENT-MIB, which is available at www.sourceforge.net. Traps in this class are handled by the NMS to detect changes in the state of the elements.

Trap description

The SNMP trap description provides the information about the type of error that occurs on the system which causes the trap to be generated. Refer to *Software Input/Output System Messages (NN43001-712)*. The classification is based on the event category, such as ITG or ITS.

Software Input/Output System Messages (NN43001-712) also provides a list of critical traps that should be monitored by an SNMP monitoring system and which messages are sent as SNMP traps.

Trap format

This section describes the SNMP trap message format.

SNMPv1 message format

The SNMP traps generated from each element of the system are in SNMPv1 message format. A common trap MIB is defined so that traps from all elements are in a common format.

SNMPv1 messages contain two sections:

- message header
- Protocol Data Unit (PDU)

Message header

The message header has two fields:

- version number – specifies the version of SNMP used.
- community name – defines the members of an administrative domain and provides a simple method to control access. For more information, see "Community strings" (page 39).

Trap PDU

The trap PDU has eight fields:

- Enterprise – identifies the managed object type that generates the trap.
- Agent address – identifies the IP address of the managed object that generates the trap.

Copyright © 2007, Nortel Networks

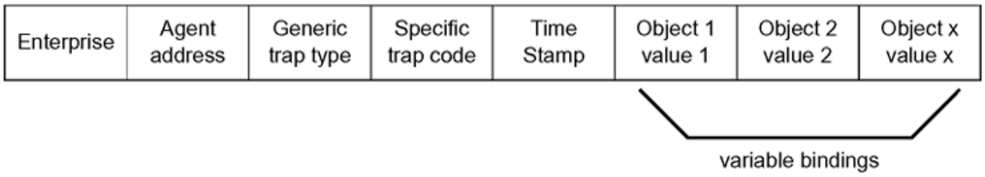
- Generic trap type – identifies the generic trap type.
- Specific trap code – identifies the specific trap code.
- Time stamp – identifies how much time elapses between when the last network initialization occurs and when the trap is generated.
- Variable bindings – identifies the data field. A variable binding associates a specific object instance with its current value. The value is ignored for the **`Get`** and **`GetNext`** commands.

See "SNMPv1 trap PDU fields" (page 59).

The number of digits in a system message code is usually three or four digits, but it can vary. Some message categories (the alphabetic portion of the system message identifier) have a variable number of digits, even for the same message category and can have either three or four digits in the output.

A message with three digits is converted to the four-digit format by adding a leading zero to the numeric portion of the message. For example, *SRPT194* is changed to *SRPT0194*. For more information about system messages, see *Software Input/Output System Messages (NN43001-712)*.

SNMPv1 trap PDU fields



Trap handling process

"Trap handling process" (page 59) describes the trap handling process.

Trap handling process

Step	Description
1	The SNMP agent on all devices, including those on Linux systems, receives information about the alarm generated on the node.

Copyright © 2007, Nortel Networks

Step	Description
2	The SNMP agent generates the SNMP trap and sends the trap to the designated IP addresses on the LAN.
3	Alarms generated as SNMP traps can sometimes generate a message to the serial port which are recorded in the log file. ***Note:*** Certain alarms on the Call Server are sent only to the serial port and are not generated as SNMP traps.

IP Telephony traps

The Signaling Server, Voice Gateway Media Card, and MGC issue specific trap types, such as ITG, ITS, and QOS. All other categories of traps are issued by the Call Server.

IP Phones do not support SNMP traps; however, the phones can cause ITS traps that are reported through the Signaling Server.

ITG and ITS trap numbering format

The numbering format of the ITG and ITS trap is ITGsxxx or ITSsxxx, where sxxx is a four-digit number (for example, ITG3021).

The first digit of the four-digit number in the error message represents the severity category of the message. The severity categories are:

1 = Critical
2 = Major
3 = Minor
4 = Warning
5 = Cleared
6 = Indeterminate

> ***Note:*** Message numbers beginning with zero do not follow this format.

For a detailed list of the ITG and ITS error messages, see *Software Input/Output System Messages (NN43001-712)*.

Viewing system error messages

When an error or specific event occurs, in most cases, an alarm trap is sent to the configured SNMP trap destinations in the IP Telephony Card properties. In every case, the system error message is written into the error log file.

Three event categories of alarm traps sent by IP Telephony devices exist:

- ITG

Copyright © 2007, Nortel Networks

- ITS
- QOS

View system error messages in CS 1000 systems

In CS 1000 systems, a system error message is issued from the Signaling Server, Voice Gateway Media Card, or MGC and written into the error log file. View the error log file by using the CLI or Element Manager.

> ***Note:*** The system log file for a Voice Gateway Media Card or other IP Telephony device can also be viewed in any text browser after the file is uploaded to an FTP host by using the `LogFilePut` command.

Viewing the error log file using Element Manager Use Element Manager to view the alarm and Exceptionlog histories and the resident system reports for the following devices:

- Signaling Server
- Voice Gateway Media Cards
- Media Gateway Controllers

For more information about viewing logs and faults, see *Element Manager System Administration (NN43001-632)*.

Corrective actions

For information about problem detection and fault-clearing actions, see the following:

- *Communication Server 1000M and Meridian 1 Small System Maintenance (NN43011-700)*
- *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*
- *Communication Server 1000E Maintenance (NN43041-700)*
- *Software Input/Output System Messages (NN43001-712)*

Troubleshooting traps

This sections describes some suggestions for troubleshooting potential missing alarms.

Potential missing alarms

If the system has SNMP enabled, and the traps are not being received by the network management system, several possible causes and solutions exist.

- Check the provisioning to ensure that the correct IP address of the trap destination is configured on the system.

Copyright © 2007, Nortel Networks

- Use the CLI on the Call Server to see if the trap has a lesser severity than the minimum severity threshold. Use the **PRT SUPPRESS_ALARM** command to determine the setting of the threshold, and the view the EPT/EDT to determine the severity of the trap.
- SNMP traps are sent over UDP protocol, which does not guarantee delivery when the network is congested.
- Traps can be discarded or not accepted for several reasons, including network congestion, the SNMP Manager(s) not having the correct trap MIB loaded, or the SNMP Manager not being able to process the trap.
- Traps can be suppressed if issued too frequently.

Copyright © 2007, Nortel Networks

MIBs

Contents

This chapter contains information about the following topics:

Overview

When using typical IP network devices, the operator requires a large amount of management information to properly run the device. This information is kept on the system and can be made available to network management systems through SNMP. The information itself is kept on the device (conceptually) in a database referred to as a Management Information Base (MIB). The network management system can query the MIB through SNMP query commands (called `gets`), and in some cases, can modify the MIB through SNMP `set` commands.

> ***Note:*** The SNMP `set` commands to the MIB-II Group variables (for example, sysLocation, sysContact, and sysName) are not supported. The System Group variables are only configured through a management interface, such as Element Manager, and not with SNMP.

For the Network Management System (NMS) to communicate with the agent on a managed device, the NMS must have a description of all manageable objects that the agent knows about. Therefore, each type of agent has an associated document called a MIB Module that contains these

Copyright © 2007, Nortel Networks

descriptions. MIB Module files are loaded into the NMS. MIB Modules are frequently referred to as MIBs. The primary purpose of the MIB module is to provide a name, structure, and a description for each of the manageable objects that a particular agent knows about.

Two kinds of MIB modules are used by the NMS:

- a generic MIB Module that describes the structure of the data that the NMS can retrieve
- a trap MIB Module that describes the structure of the data sent by the device agent as an SNMP trap

MIB data is arranged in a tree structure. Each object (each item of data) on the tree has an identifier, called an Object ID (OID), that uniquely identifies the variable. To prevent naming conflicts and provide organization, all major device vendors, as well as certain organizations, are assigned a branch of this tree structure referred to as the MIB Tree. The MIB Tree is managed by the Internet Assigned Numbers Authority (IANA). Each object on the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name.

An SNMP MIB must be written in ASN.1 format to conform with the SNMP standards.

ASN.1

ASN.1 stands for Abstract Syntax Notation version 1. ASN.1 is a standard regulated by the International Organization for Standardization (ISO) that defines the nodes (branches) of the MIB tree in a numeric manner. The path is designated by periods (.) rather than slashes (/), like those used in a directory path for files on a PC.

Example: .1.3.6.1.2.1.1.3

"First four ASN.1 Object Types" (page 64) lists the Object Types for the first four numbers of an OID that uses ASN.1 syntax.

First four ASN.1 Object Types

Number	Object Type	Description
1	iso	International Organization for Standardization.
2	org	Everything under this branch is an organization recognized by the ISO.
3	dod	Department of Defense.
4	internet	The node allocated by the DOD for the Internet community.

Copyright © 2007, Nortel Networks

Below the internet node are four defined named nodes:

- directory(1)
- mgmt(2)
- experimental(3)
- private(4)

For most MIB objects on IP devices, the first four numbers are always .1.3.6.1.

After the first four numbers two main nodes (or branches) are used on IP devices:

1. mgmt(2) node – where the MIBs that are defined by standards organizations are found.
2. private(4) node – where vendors, such as Nortel, define their own private (or enterprise) MIB modules. Each vendor has a unique number assigned to it, therefore, the OID for any object uniquely identifies which vendor has implemented the MIB. The vendor ID for Nortel is 562.

Named nodes

Nodes are given both a number and a name. Mgmt is node two and private is node four. The OID is written with the node number in parentheses next to the Object Type.

Example: iso(1) org(3) dod(6) internet(1) mgmt(2)

that is equivalent to the numerical OID string of:

.1.3.6.1.2

The child node of mgmt(2) is mib(1). Many child nodes are under the mib(1) node. These child nodes represent related groups of internet protocols or concepts. If an SNMP agent supports a particular group, the agent is said to be compliant for that group.

Below the management category are several groups of management objects, including the following:

- system(1)
- interfaces(2)
- at(3)
- ip(4)
- icmp(5)

Copyright © 2007, Nortel Networks

system group

The system group contains objects that describe some basic information about the SNMP agent or the network device object on which the agent is running. The combined agent and network device object is referred to as the entity. "system objects" (page 66) lists some of the common objects in the system group.

system objects

Object	Description
sysDescr	Description of the entity.
sysObjectID	Complete OID string defined by the vendor that created the entity. This object is used extensively by TM (and other SNMP applications) to quickly identify what kind of SNMP agent the application is talking to.
sysUpTime	Time (in hundredths of a second) since the network management portion of the system is last reinitialized.
sysContact	Contact person – usually the name of the person locally responsible for the entity.
sysName	Navigation Site Name: Navigation System Name: <HostName>.
sysLocation	System location.

Configuring the sysDescr OID string

The System group MIB contains a sysDescr OID with a specific format. The following sections describe the format in detail.

sysDescr string format PR:`"<product name>"` SW:`"<main application>"` BN:`"<full release number>"` HW:`"<hardware name>"` FW:`"<firmware version>"` (c) Nortel Networks

> ***Note:*** A co-resident VxWorks NRS is classified as a Signaling Server.

The format is a name-value pair of all applicable attributes, with the value portion enclosed in quotes for ease of parsing. You can omit attributes that do not apply, therefore firmware information (FW:) appears only for some Voice Gateway Media Cards. For example, firmware information appears for ITG-P and ITG-SA, but not for MC32S.

Where PR: is one of the following:

- Meridian 1
- CS 1000
- CS 1000M
- CS 1000E

Copyright © 2007, Nortel Networks

Note: CS 1000E is the product name for MG 1000E.

Where SW: is one of the following:

- Call Server, Sys XXXX
- MG 1000B - Call Server, Sys XXXX
- Signaling Server
- VGMC
- Expansion Call Server - Normal mode, Sys XXXX
- Expansion Call Server - Survival mode, Sys XXXX
- MGC
- MG 1000E-SSC
- NRS for Linux NRS/GK
- ECM for Linux ECM

Note 1: If multiple applications are on the server, SW: pertains to the main use of the server.

Note 2: NRS on VxWorks is classified as Signaling Server.

Where BN: is one of the following:

- X.XXY for CS
- sse-X.XX.XX for SS
- IPL-X.XX.XX for VGMC
- mgcYYYXX for MGC
- X.XX.XX for NRS/ECM on Linux (application CD version number)

Note: In the BN: value fields, X is a value from 0 to 9 and Y is a value from a to z.

Where HW: is one of the following:

- CP-P2
- CP-P4
- CP-PM (Call Server)
- CPPM (Signaling Server)
- SSC
- ISP1100
- ITG-P

Copyright © 2007, Nortel Networks

- ITG-SA
- MGC
- MC32S
- HP DL320 for NRS/ECM on Linux
- IBM 306M for NRS/ECM on Linux
- HP-DL320-G4 for SS COTS
- IBM-x306m for SS COTS

Examples:

PR: `"CS 1000E"` SW: `"Call Server, Sys 4021"` BN: `"4.91F"` HW: `"CP-PM"` (c) Nortel Networks.

PR: `"CS 1000"` SW: `"NRS"` BN: `"4.91.05"` HW: `"IBM 306M"` (c) Nortel Networks.

Example of an OID string

The OID string for the sysUpTime object is:

iso(1) org(3) dod(6) internet(1) mgmt(2) mib(1) system(1) sysUpTime(3)

or

.1.3.6.1.2.1.1.3

MIB abbreviations

Another way to write the previous example is:

::= { system 3 }

system(1) is already known as iso(1) org(3) dod(6) internet(1) mgmt(2) mib(1) system(1) or .1.3.6.1.2.1.1. It is only necessary to define how the sysUpTime object fits into the preexisting structure.

::= represents the .1.3.6.1.2.1 portion of the MIB.

The third object in the system(1) group is the sysUpTime object; therefore, it is defined as { system 3}.

OID queries

If an OID string is not complete down to the object—that is, if the string ends at a node instead of a specific object—this affects the results when the OID string is queried.

Copyright © 2007, Nortel Networks

Example

.1.3.6.1.2.1.1

is equivalent to

iso(1) org(3) dod(6) internet(1) mgmt(2) mib(1) system(1)

If the string is queried, it returns the value for sysDescr, sysObjectID, sysUpTime, sysContact, and all the other objects within the system(1) node.

Variable binding

Variable binding is the pairing of an SNMP object instance name with an associated value. A variable binding list is a series of variable binding entries.

Supported MIBs

"Supported MIBs" (page 69) lists the MIBs supported on the CS 1000 and Meridian 1 systems. There is no difference between the enterprise-specific MIBs for Meridian 1 and CS 1000 systems, except that there are no Signaling Server MIBs on Meridian 1 systems.

Supported MIBs

	MIB-II groups	Other
Call Server	• System group (RFC 1213) • Interface group (RFC 2863) • IP group (RFC 2011) • UDP group (RFC 2013) • TCP group (RFC 2012) • ICMP group (RFC 2011) • SNMP group (RFC 3418) • Entity group (RFC 2737) (only the following two subgroups) — Physical — General • Host Resources group (RFC 2790) (only the following subgroups) — hrSystem group — hrStorage group	• Nortel Proprietary MIBs

Copyright © 2007, Nortel Networks

	MIB-II groups	Other
	— hrDevice group — hrSWRun group — hrSWRunPerf group ***Note:*** Only certain objects in the Host Resources subgroups are supported.	
Signaling Server, Voice Gateway Media Cards, and Media Gateway Controllers	• System group (RFC 1213) • Interface group (RFC 2863) • IP group (RFC 2011) • UDP group (RFC 2013) • TCP group (RFC 2012) • ICMP group (RFC 2011) • SNMP group (RFC 3418) • Host Resources group (RFC 2790) (only the following subgroups) — hrSystem group — hrStorage group — hrDevice group — hrSWRun group — hrSWRunPerf group ***Note:*** Only certain objects in the Host Resources subgroups are supported.	• QOS-MIB.mib ***Note:*** QOS-MIB.mib is also known as Zonetrafficrpt MIB - Signaling Server only.

"Definition of MIBs" (page 70) defines the various MIBs.

Definition of MIBs

MIB	Definition
Call Server MIB	

Copyright © 2007, Nortel Networks

MIB	Definition
System group	Provides information about the system name, location, contact, description, object ID, and uptime. Only the System group can be provisioned. All the other groups are read-only. The following OIDs are supported: sysDescr, sysObjectID, sysUpTime, sysContact, sysName, and sysLocation. The default values for the system group are: **sysDescr:** See "Configuring the sysDescr OID string" (page 66) for a description and examples of the sysDecscr OID. **sysObjectID:** `.1.3.6.1.4.1.562.3`(.iso.org.dod.internet.private.enterprises.nt.meridian) **sysContact:** System Contact **sysName:** Navigation Site Name: <HostName> **sysLocation:** System Location
Interface group	Provides information about the network interfaces on the system, such as description, physical address, and speed. Also provides statistics and data, such as the number of in/out packets and discarded packets.
IP group	Provides information about the IP stack, such as default TTL and IP addresses. No provisioning is required for this group. The SNMP agent gathers this information automatically.
UDP group	Provides information about the UDP stack, such as UDP port numbers and errors.
TCP group	Provides information about the TCP stack, such as routing algorithm and TCP port numbers.
ICMP group	Consists of counters that measure the rates at which Internet Control Message Protocol (ICMP) messages are sent and received using ICMP protocol. It also includes counters that monitor ICMP protocol errors.

Copyright © 2007, Nortel Networks

MIB	Definition
SNMP group	A collection of objects providing basic information and control of an SNMP entity, such as: • total number of messages delivered to the SNMP entity from the transport service • total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version
Entity group	Provides information about the physical inventory of the system, such as component information, relationships between components, and relationships to logical interfaces. The following groups of the Entity MIB are supported: • Entity Physical Group: provides information about the hardware components such as description, vendor type, and name and covers the following objects: — entPhysicalDescr — entPhysicalVendorType — entPhysicalContainedIn — entPhysicalClass — entPhysicalParentRelPos — entPhysicalName — entPhysicalHardwareRev — entPhysicalFirmwareRev — entPhysicalSoftwareRev — entPhysicalSerialNum — entPhysicalMfgName — entPhysicalModelName — entPhysicalAlias — entPhysicalAssetID — entPhysicalFRU • Entity General Group: provides information about the last time any changes are made in the Entity Physical Group, in the format of sysUpTime. Entity General Group covers the following object: — entLastChangeTime

Copyright © 2007, Nortel Networks

MIB	Definition
Host Resources group	Defines a uniform set of objects useful for the management of host devices. The host devices are independent of the operating system, network services, and software applications. The Host Resources MIB lets a Network Management System (NMS) obtain information about the host device, including the following: • system properties • memory management and utilization • devices attached to the host device and details about the attached devices • performance of the applications on the host device The following subgroups are supported: hrSystem Group, hrStorage Group, hrDevice Group, hrSWRun Group, and hrSWRunPerf Group. **hrSystem Group:** • hrSystemUptime Amount of time since the host (Call Server) is last initialized. Shows the time elapsed since the host is last rebooted. The value is in the form of time ticks elapsed and is determined by comparing the present local time and the time when the Call Server is last warm- or cold-booted. • hrSystemDate Date and time presently shown by the Call Server, displayed in octet format. • hrInitialLoadDevice The device from which the host (Call Server) is booted. The return value is always one because the Call Server always boots from the Hard Disk. • hrInitialLoadParameters Parameters supplied to the device while the host is booted. The path of the file from which the Call Server boots is provided. • hrSystemNumUsers Number of user sessions for which the host (Call Server) stores the state information; that is, how many rlogin sessions are presently occupied in the Call Server. • hrSystemProcesses List of process contexts currently loaded or running on the Call Server. For example, it lists the tasks such as ttimer, tSNMP, and tScriptMgr that are presently running in the Call Server. • hrSystemMaxProcess The maximum number of tasks that the Call Server can support at the same time.

Copyright © 2007, Nortel Networks

MIB	Definition
	hrStorage Group: • hrMemorySize Amount of physical RAM in the Call Server in units of Kilobytes. • hrStorageTable Table of logical storage areas on the host, as seen by an application. A useful diagnostic for *out of memory* and *out of buffers* types of failures. — hrStorageIndex A unique value for each logical storage area contained by the host. — hrStorageType Type of storage. Storage types can be Flash Memory, RAM, or PC Card. Value is returned as hrStorageRam or hrStorageFlashMemory for the Call Server, depending on what storage types are present. — hrStorageDescr Name of the storage device. All storage devices available in the Call Server are listed. — hrStorageAllocationUnits Size, in bytes, of the data objects allocated from this pool. If this entry is monitoring sectors, blocks, buffers or packets, for example, this number is usually greater than one. Otherwise, this value is typically one. Example of a return value is 65536 bytes for virtual memory. — hrStorageSize Size of storage in units of hrStorageAllocationUnits. — hrStorageUsed Storage that is allocated in units of hrStorageAllocationUnits. Value is the memory utilized given in hrStorageAllocationUnits. — hrStorageAllocationFailures Always returns a value of zero. Nortel recommends that you use the following space utilization thresholds when you monitor disk drives. Values greater than these can result in system problems. • /d, /u: 85% (/d is the real partition name; software uses /u), used for data storage and patching • /e: 85%, logging and temporary space for the CCBR back-up compression process • /boot: boot partition, no need to monitor • /p: protected partition for software installation, no need to monitor

Copyright © 2007, Nortel Networks

MIB	Definition
	• cd0: cd drive, no need to monitor • f0: floppy drive, no need to monitor • /cf2: face plate compact flash, no need to monitor • SSC c: 85% • SSC z: 85%, this is an archive drive. The drive is formatted before it is used. The database is copied, then patches (where patch copy is best effort) until the drive is full. • SSC a: PCMCIA a, do not monitor • SSC b: PCMCIA b, do not monitor **hrDevice Group:** Useful for identifying and diagnosing the devices on a system. In addition, some devices have device-specific tables for more detailed information. • hrDeviceTable Conceptual table of devices contained by the host. — hrDeviceIndex A unique value for each device contained by the host. — hrDeviceType Type of device associated with the host. Example is hrDeviceProcessor for which a corresponding conceptual table is created called hrProcessorTable. — hrDeviceDescr Textual description of this device. This description is the same as that of sysDescr in the System group MIB. — hrDeviceID Product ID of the device attached to the host (Call Server). This ID is the same as that of sysObjectid in the System group MIB. — hrDeviceStatus Current status of the device. — hrDeviceError Error value in the device. Output is zero if the device is running. • hrDiskStorageTable — hrStorageIndex Unique value for each logical storage device contained by the host.

Copyright © 2007, Nortel Networks

MIB	Definition
	— hrDiskStorageAccess Indicates if the fixed storage device in the Call Server is read/write or read-only. — hrDiskStorageMedia Type of media used in the long-term storage device in Call Server. It can be hard disk, floppy disk, or CD-ROM. — hrDiskStorageRemoveable Disk Storage removal indication. Indicates whether the storage media can be removed from the Call Server. For example, the CD-ROM can be removed from Call Server, so its return value is *true*; the hard disk cannot be removed, so its return value is *false*. — hrDiskStorageCapacity Total size of the storage media. If the storage media is removable and is currently removed, the value is zero. • hrProcessorTable Table of processors contained by the host. — hrProcessorFrwID Product ID of the firmware associated with the processor. The object identifier of the Call Server is used for this object value. — hrProcessorLoad An idle task on the Call Server takes up spare CPU cycles, so a raw CPU utilization value is always 100%. Instead of using a raw CPU utilization value, the value returned for hrProcessorLoad is the percentage of the rated call capacity used during a 30 second interval. This value is not available until 24-hours after a system restart, because the percentage of the rated call capacity is calculated over a 24-hour period. In that 24-hour window, only negative values are returned until the correct value is available. There may be other conditions under which the rated call capacity cannot be computed. For example, continuous heavy traffic load on the system can produce insufficient cycles to determine the rated call capacity; this causes negative values to be returned. Rated call capacity is 70% of peak call capacity; therefore the hrProcessorLoad value could exceed 100% in heavy load conditions. Due to the nature of the statistical computation of the rated call capacity and the short period of measurement, values significantly higher than 100% can be seen at times (for example, 300%). This can be the result of a large number of calls during the 30 second interval of measurement. Traffic report TFS004 gives a measurement of the percentage of call capacity used over a period of an hour and should be examined if hrProcessorLoad returns unusually high values. TFS004 is a more reliable measure of processor usage.

Copyright © 2007, Nortel Networks

MIB	Definition
	Measurements in excess of 80% on a sustained basis (for example, after the system runs on a stable basis for some time) can require action, and sustained measurements of over 100% can lead to outages. For more information about rated call capacity see the TFS004 Processor Load documentation in *Traffic Measurement Formats and Output Reference (NN43001-750)*.
	hrSWRun Group: • hrSWRunTable Contains an entry for each distinct piece of software that is running or loaded into physical memory in preparation for running. Includes the operating system, device drivers, and applications of the host device. — hrSWRunIndex Unique value for each piece of software running on the host, displayed as sequential integers. — hrSWRunName Textual description of this running piece of software, including the name by which it is commonly known. — hrSWRunID Product ID of this running piece of software (similar to hrSWRunIndex). — hrSWRunType Type of software. Values are unknown(1), operatingSystem (2), deviceDriver(3), and application(4). — hrSWRunStatus Status of this running piece of software. Values are: 1. running(1) 2. runnable(2) but waiting for resource (such as CPU, memory, IO) 3. notRunnable(3) – loaded but waiting for event 4. invalid(4) – not loaded ***Note:*** Values are read-only.

Copyright © 2007, Nortel Networks

MIB	Definition
	hrSWRunPerf Group: Contains an entry corresponding to each entry in the hrSWRunTable. To implement the hrSWRunPerf Group, the hrSWRunGroup must be supported. • hrSWRunPerfCPU Number of centi-seconds of CPU resources consumed by the Call Server for this process. • hrSWRunPerfMemory Total amount of the real memory allocated to the Call Server for this process.
Signaling Server MIB	
System group	Provides information about the system contact, description, and object ID. Only the System group can be provisioned. All the other groups are read-only. The default values for this system group are: The following OIDs are supported: sysDescr, sysObjectID, and sysContact. The default values for the system group are: **sysDescr:** See "Configuring the sysDescr OID string" (page 66) for a description and examples of the sysDecscr OID. **sysObjectID:** `.1.3.6.1.4.1.562.3.21` (.iso.org.dod.internet.private.enterprises.nt.meridian.sigserv) **sysContact:** System Contact
Interface group	See the Call Server MIB Interface group description in this table.
IP group	See the Call Server MIB IP group description in this table.
UDP group	See the Call Server MIB UDP group description in this table.
TCP group	See the Call Server MIB TCP group description in this table.
ICMP group	See the Call Server MIB ICMP group description in this table.
SNMP group	See the Call Server MIB SNMP group description in this table.

Copyright © 2007, Nortel Networks

MIB	Definition
Host Resources group	See Call Server MIB Host Resource group description in this table (all references to the host or Call Server are considered to be references to Signaling Server). ***Note 1:*** hrProcessorTable is not supported on the Signaling Server. ***Note 2:*** In the hrSystem group, the hrSystemNumUsers value describes the number of connection sessions (for example, Telnet, Rlogin, SSH, FTP).

QOS MIB group	Defined by QOS-MIB.mib. Presents the QOS-related data from LD 2, System Traffic Report 16.
	For information about the System Traffic Report 16, see *Traffic Measurement Formats and Output Reference (NN43001-750)* (NN43001-750).
	Note: The QOS-MIB.mib is also known as the Zonetrafficrpt.mib.
	The QOS-MIB.mib consists of traffic parameters for zones provisioned on the Call Server. There are two sets of parameters: intrazone parameters and interzone. Each parameter is assigned an Object ID in the MIB.
	The QOS-MIB.mib is a part of the NT node and subtends off the Signaling Server in the object ID tree structure. The object ID sequence for the QOS group MIB is .1.3.6.1.4.1.562.3.21.6.
	QOS MIB Access Setup
	Create a Limited Access Password (LAPW) user account on the system for QOS MIB access to the Signaling Server. Set the account user name to **snmpqosq**. Set the account password to any appropriate password.
	Note: For greater security, the account is limited to access only LD 117.
	Follow these steps to create the LAPW user account:
	1. Log on to the CLI using the Level 2 account.
	At the prompt, enter LD 17 and respond to the prompts as follows:
	`REQ chg`
	`TYPE pwd`
	`..`
	`..`
	`ACCOUNT_REQ NEW`
	`PWD_TYPE LAPW`
	`PWTP ovly`
	`USER_NAME snmpqosq`
	`PASSWORD anypass`
	`CONFIRM anypass`
	`OVLA 117`
	`..`

Copyright © 2007, Nortel Networks

MIB	Definition

	`..`
	`PWD ACCOUNT SETTINGS SAVED`
	Note: Accept default value for prompts that are not shown. The term anypass refers to any appropriate password.
	2. Verify the user account is created correctly by logging on to the CLI with the LAPW user account and accessing overlay 117.
	3. Verify access to the Signaling Server QOS MIB using any SNMP tool and the ADMIN_COMM(2) configured community string (the OID branch is .1.3.6.1.4.1.562.3.21.6).
	4. Use LD 02 or Element Manager to view System Traffic Report 16 and ensure the same values are returned using the QOS MIB query.
	The QOS-MIB.mib utilizes a LD 117 command to populate the data in the MIB. LD 117 supports only one user with the **`MULTI_USER LOGIN`** option enabled. Therefore, if LD 117 is in use, either through the CLI at a TTY port or through Element Manager, an SNMP query to the QOS-MIB.mib fails, as the query does not have access to the overlay. A syslog message indicating that the overlay memory space is in use is displayed on the Signaling Server.
	Note: There must be Pseudo-TTY (PTY) ports configured and available on the Call Server for the SNMP query to succeed.
	The implementation of the QOS-MIB.mib involves caching information and entails delays at times. When an attribute is fetched (for example, `callsMadeIn`), the values for all zones are retrieved internally and cached. The most efficient method is to retrieve the table is by using successive **`GETNEXT`** requests, which retrieve values for all zones in sequence. When you move to a new attribute on any request there is a delay of three seconds or longer, but the retrieval of the attribute value for successive zones (after zone zero) is immediate. Other patterns of retrieval, such as **`GET`** operations for each attribute and zone, can result in longer overall retrieval times.

Voice Gateway Media Card MIB	

Copyright © 2007, Nortel Networks

MIB	Definition
System group	Provides information about the system name, contact, description, and object ID. Only the System group can be provisioned. All the other groups are read-only. The following OIDs are supported: sysDescr, sysObjectID, sysContact, and sysName. The default values for the system group are: **sysDescr:** See "Configuring the sysDescr OID string" (page 66) for a description and examples of the sysDescr OID. **sysObjectID:** `.1.3.6.1.4.1.562.3.11.5`(.iso.org.dod.internet.private.enterprises.nt.meridian.itg.iplmib) **sysContact:** System Contact **sysName:** <Voice Gateway Media Card host name> <TN>
Interface group	See the Call Server MIB Interface group description in this table.
IP group	See the Call Server MIB IP group description in this table.
UDP group	See the Call Server MIB UDP group description in this table.
TCP group	See the Call Server MIB TCP group description in this table.
ICMP group	See the Call Server MIB ICMP group description in this table.
SNMP group	See the Call Server MIB SNMP group description in this table.
Host Resources group	See the Call Server MIB Host Resource group description in this table (all references to the host or Call Server are considered to be references to the Voice Gateway Media Card). ***Note 1:*** In the hrSystem group, the hrSystemNumUsers value describes the number of connection sessions (for example, Telnet, Rlogin, SSH, FTP). ***Note 2:*** In hrStorage Group, the hrStorageUsed object returns the utilized memory in hrStorageAllocationUnits. For Voice Gateway Media Cards, the output is minus one because no storage-related library for obtaining the free storage is exposed. ***Note 3:*** hrProcessorTable is not supported on the Voice Gateway Media Card.
Media Gateway Controller (MGC)	

Copyright © 2007, Nortel Networks

MIB	Definition
System group	Provides information about the system description, object ID, and contact. Only the System group can be provisioned. All the other groups are read-only. The following OIDs are supported: sysDescr, sysObjectID, and sysContact. The default values for the system group are: **sysDescr:** See "Configuring the sysDescr OID string" (page 66) for a description and examples of the sysDecscr OID. **sysObjectID:** `.1.3.6.1.4.1.562.3.7` (.iso.org.dod.internet.private.enterprises.nt.meridian.mgc) **sysContact:** System Contact
Interface group	See the Call Server MIB Interface group description in this table.
IP group	See the Call Server MIB IP group description in this table.
UDP group	See the Call Server MIB UDP group description in this table.
TCP group	See the Call Server MIB TCP group description in this table.
ICMP group	See the Call Server MIB ICMP group description in this table.
SNMP group	See the Call Server MIB SNMP group description in this table.
Host Resources group	See Call Server MIB Host Resource group description in this table (all references to the host or Call Server are considered to be references to the MGC). ***Note 1:*** hrProcessorTable is not supported on the MGC. ***Note 2:*** In the hrSystem group, the hrSystemNumUsers value describes the number of connection sessions (for example, Telnet, Rlogin, SSH, FTP).
Linux NRS and ECM	
System group	Provides information about the system name, location, contact, description, object ID, and uptime. Only the System group can be provisioned. All the other groups are read-only. The following OIDs are supported: sysDescr, sysObjectID, sysContact, sysName, and sysLocation. The default values for the system group are: **sysDescr:** See "Configuring the sysDescr OID string" (page 66) for a description and examples of the sysDecscr OID. **sysObjectID:** For NRS: .1.3.6.1.4.1.562.3.12

Copyright © 2007, Nortel Networks

MIB	Definition
	(.iso.org.dod.internet.private.enterprises.nt.meridian.nrs) For ECM: .1.3.6.1.4.1.562.3.13 (.iso.org.dod.internet.private.enterprises.nt.meridian.ecm) **sysContact:** System Contact **sysName:** System Name **sysLocation:** System Location
Interface group	See the Call Server MIB Interface group description in this table.
IP group	See the Call Server MIB IP group description in this table.
UDP group	See the Call Server MIB UDP group description in this table.
TCP group	See the Call Server MIB TCP group description in this table.
ICMP group	See the Call Server MIB ICMP group description in this table.
Interface group	See the Call Server MIB SNMP group description in this table.
Host Resources MIB	The default implementation of the HR MIB supplied by the Net-SNMP agent is used. ***Note:*** hrProcessorTable is not supported on Linux.

Entity group MIB

At system startup, the Entity MIB receives information about all system hardware (such as common equipment, loops, cards, IP Phones) detected and configured in the system. If a Midnight Routine is configured in LD 117 (**`INV MIDNIGHT SETS/CARDS/ALL/NONE`**), then the MIB is updated daily as part of the Midnight Routine inventory.

If the Midnight Routine inventory is configured only for IP Phones (**`SETS`**), then only inventory information on IP Phones is updated daily; if only configured for cards, then only card inventory information is updated daily. If the Midnight Routine inventory is configured for all devices, then all inventory information is updated. If the Midnight Routine is not configured at all, no updates to the Entity MIB are made.

The Entity MIB is updated immediately if an IPE card is inserted or removed or if an IP Phone registers or unregisters from the Call Server.

When one of these hardware changes is detected, the inventory of the corresponding hardware entities is completely updated. For example, if an IP Phone registers or unregisters, the inventory for all telephones (digital telephones and IP Phones) is updated. If a Digital Line Card is removed, the inventory for all cards (and loops, common equipment, and so on) is updated.

Copyright © 2007, Nortel Networks

The inclusion of the telephones in the Entity MIB is configured in LD 117. See "LD 117 telephone inventory in Entity MIB command" (page 84).

LD 117 telephone inventory in Entity MIB command

=> Command	Description
INV ENTITY SETS	
ON	Turns ON the inclusion of digital telephones and IP Phones in the Entity MIB.
(OFF)	Turns OFF the inclusion of digital telephones and IP Phones in the Entity MIB.
STATUS	Displays whether or not the digital telephones and IP Phones are included in the Entity MIB. Either ON or OFF appears in the output.

Accessing MIBs

ATTENTION

The CS 1000 Release 5.0 enterprise-specific MIBs are

- COMMON-TRAP-MIB.mib
- QOS-MIB.mib (also known as the Zonetrafficrpt.mib)

Download the latest version of the MIBs for Nortel products from www.nortel.com.

Follow the steps in "Downloading the MIBs from the Nortel Web site" (page 84) to download the MIBs.

Downloading the MIBs from the Nortel Web site

Step Action

1 Under the **Support & Training** banner, choose **Technical Support > Software Downloads**.

2 Click the **Browse product support** tab.

3 In **1. Select From**, choose a product family.

Meridian 1 and CS 1000 MIBs are found under **Communication Servers - Enterprise Communication Servers**.

The TM OpenAlarm MIB is found in the **Optivity** family of products.

4 In **2... Select a product**, choose a system type.

Copyright © 2007, Nortel Networks

5 In **3... and get the content**, choose **Software**.

6 The MIBs are found in the downloadable software list.

—End—

Trap handling approaches

Three approaches are available to handle traps sent from the CS 1000 and Meridian 1 devices. Nortel recommends that you use a Network Management System (NMS) to accept traps directly from the system components.

1. Use an NMS (for example, HP OpenView) to accept traps directly from the CS 1000 system components.

   To understand the structure of the traps that are sent from the system components, the NMS usually requires that the trap MIB modules are loaded into the NMS. The MIBs from each CS 1000 or Meridian 1 component must be loaded into the NMS. See the **Attention** dialog box in "Accessing MIBs" (page 84) for the required MIB modules.

   See also "Directly accepting traps with Network Management Systems and HP OpenView" (page 85).

2. Use TM to accept the traps from the system components.

   No trap MIBs are required. TM has the trap MIB structure built into its software. See "Directly accepting traps with Network Management Systems and HP OpenView" (page 85).

   For information about using TM, see *Telephony Manager 3.1 System Administration (NN43050-601)*.

3. Use an NMS to accept traps that are sent from the system components to the TM and then forwarded to the NMS by the TM Alarm notification feature.

   Only the TM OpenAlarm MIB is required on the NMS. TM remaps the structure and severity of the traps to conform to the TM OpenAlarm MIB.

Directly accepting traps with Network Management Systems and HP OpenView

This section contains information about how to accept traps directly when using NMS, HP OpenView, or third-party management systems.

Enterprise Network Management System

The Enterprise NMS can accept traps directly from the CS 1000 systems. For information about using and configuring TM to forward traps to Enterprise NMS, see *Installing Nortel Enterprise Network Management*

Copyright © 2007, Nortel Networks

System (321537-B) 10.4, *Administering Nortel Enterprise Network Management System (205969-J)* 10.4, and *Using Nortel Enterprise Network Management System (207569-G)* 10.4.

HP OpenView

The common trap MIB (**`COMMON-TRAP-MIB.mib`**) is used to enable HP OpenView to accept traps directly from the CS 1000 devices. For more information, see Appendix "Configuring SNMP alarms in HP OpenView NNM" (page 91).

Third-party NMSs

If neither Enterprise NMS or HP OpenView NMS is used, the common trap MIB must be used in the trap-handling process of the third-party NMS.

Copyright © 2007, Nortel Networks

Appendix A
Administration

Contents

This chapter contains information about the following topics:

EDT and EPT

The Event Default Table (EDT) and Event Preference Table (EPT) are repositories on the Call Server for storing system event information.

The EDT contains a list of system events and default event severities that the system generates. Each event contains an event code, a description, and severity information. Data in the EPT overrides the severity of an event assigned in the EDT. You can use the EPT to configure escalation thresholds and suppression thresholds for certain event severities.

The maximum number of entries allowed in the EPT is 500.

Use LD 117 commands to import and export an EPT file from/to removable media, to load an updated EPT file into memory, and to print the EDT and EPT entries. See "LD 117 EDT and EPT commands" (page 87).

LD 117 EDT and EPT commands

=> Command	Description
`EXPORT EPT`	The EPT file stored on the hard disk (/u/db/ smpserv.db) is copied to the floppy/PC Card drive (a:/smpserv.db).
`IMPORT EPT`	The EPT file stored on the floppy/PC Card (a:/smpserv.db) drive is copied to the hard drive (/u/db/smpserv.db).

Copyright © 2007, Nortel Networks

=> Command	Description
`RELOAD EPT`	The new/modified EPT file is loaded into memory from disk (/u/db/smpserv.db).

`PRTS EPT`
`severity <eventID> <eventID>`
	The entries in the EPT can be listed based on the severity field for all entries or the specified range of entries.

`PRTS EDT`
`severity <eventID> <eventID>`
	The entries in the EDT can be listed based on the severity field for all entries or the specified range of entries.

The EPT file is created when data is entered in the EPT and an EDD is performed. The EDD must be done prior to exporting the EPT file with the **EXP EDD** command. Error messages are issued if the import or export of the EPT file is not successful.

WARNING
When the EPT file is exported to a management workstation, the EPT file must not be modified using a text editor or spreadsheet application. If the EPT file is modified offline, it does not import correctly on the switch. The only supported way to modify the EPT file is through LD 117, Element Manager, or Telephony Manager (TM).

Backup and restore

LD 43

The LD 43 commands listed in "LD 43 backup and restore commands" (page 88) enable a backup and restore of the Call Server system group MIB variables, System Navigation variables, community strings, and other data.

LD 43 backup and restore commands

=> Command	Description
`EDD`	The Call Server system group MIB variables, System Navigation variables, community strings, Trap community strings, and other data are dumped to disk as a file when this command is executed. As well, this file is backed up to the A: drive floppy (Large Systems) or to the internal Z: drive (Small Systems).
`BKO`	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is copied from the primary device to the backup (external storage) device.

Copyright © 2007, Nortel Networks

=> Command	Description
RES	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is restored from the backup (external storage) device to the primary device.
RIB (Small Systems only)	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is restored from the internal backup device to the primary device.

LD 143

The LD 143 commands listed in "LD 143 Small System backup and restore commands using a PC Card" (page 89) are part of the LD 143 Small System Upgrade Utilities menu. Select Option 2 to archive (backup) the system group MIB variables, System Navigation variables, community strings, and other data to a PC Card.

LD 143 Small System backup and restore commands using a PC Card

=> Command	Description
2. **Archive Customer-defined databases.**	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is archived on the PC Card.
3. **Install Archived database.**	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is installed from an archive on the PC Card.

The LD 143 Large System-specific commands listed in "LD 43 Large System backup and restore commands using floppy disks" (page 89) enable the backup and restore of the system group MIB variables, System Navigation variables, community string, and other data using floppy disks.

LD 43 Large System backup and restore commands using floppy disks

=> Command	Description
ABKO	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is backed up to floppy disks.
ARES	The new file created to store the system group MIB variables, System Navigation variables, community strings, and other data is restored from floppy disks.

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Appendix B
Configuring SNMP alarms in HP OpenView NNM

Contents

This appendix contains information about the following topics:

Overview

This section provides information on how to load and configure traps in HP OpenView Network Node Manager (NNM).

Trap MIBs

The trap MIB files specify the format of the SNMP alarms that can be sent by the system devices.

By using the format information, HP OpenView can decode and display device alarm information in an easy-to-read manner.

Alarms

Alarms contain nine information fields, also known as *attributes*, as described in the MIB modules.

Copyright © 2007, Nortel Networks

Using HP OpenView to accept traps

This section contains details about how to use HP OpenView to accept traps and how to use and view the alarm logs.

Configuring events

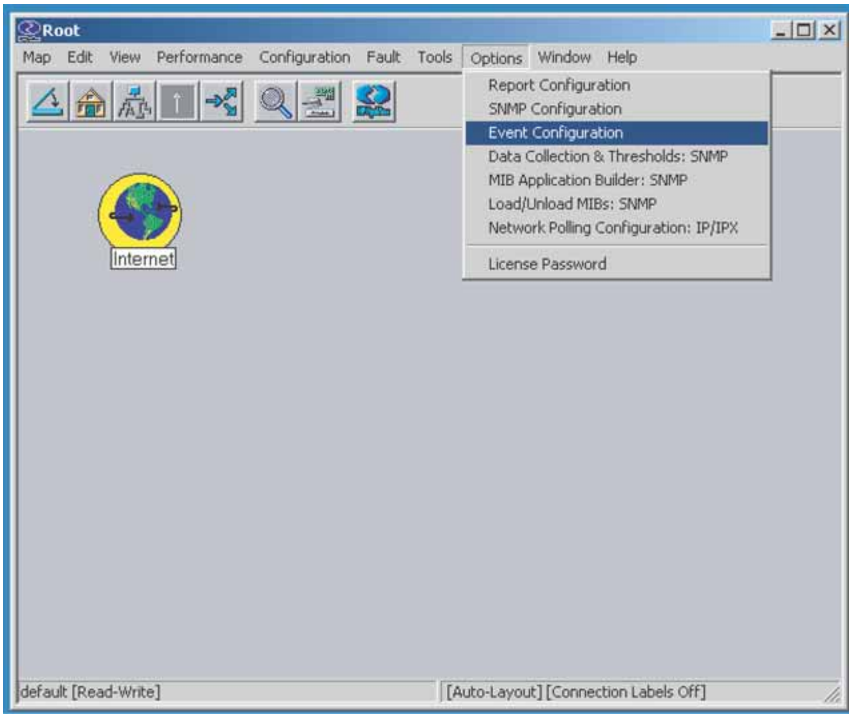
Follow the steps in "Configuring events" (page 92) to configure events in HP OpenView.

Configuring events

Step	Action
1	In the **Root** window, choose **Options > Event Configuration**.

See "Root window to Event Configuration" (page 92).

Root window to Event Configuration

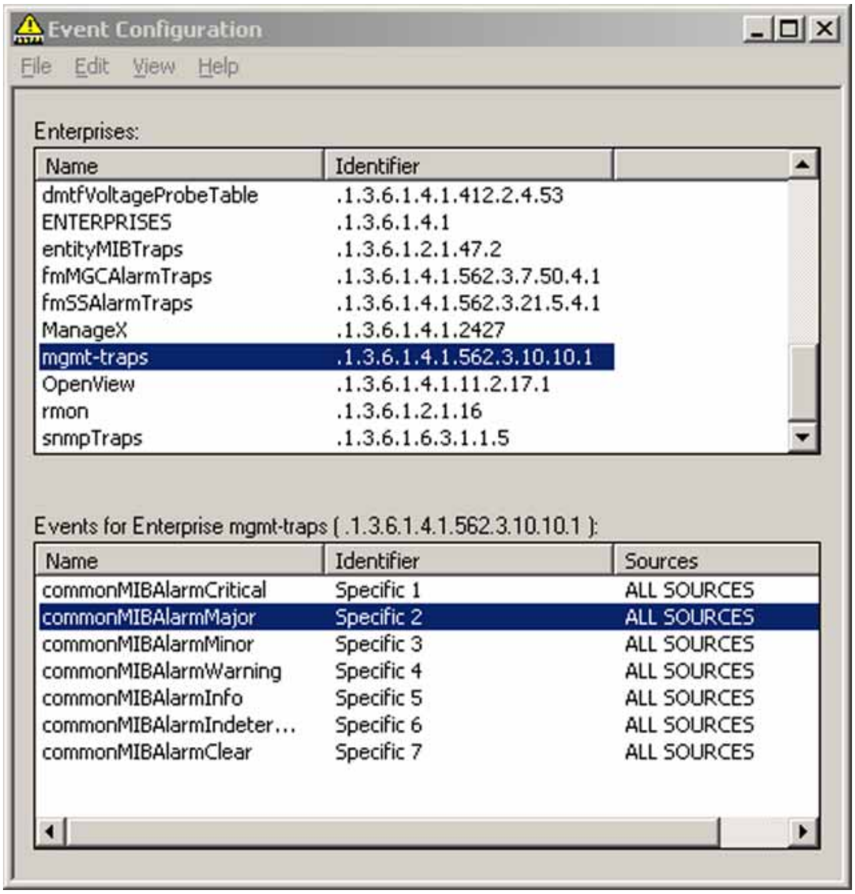

Root
Map Edit View Performance Configuration Fault Tools Options Window Help
Report Configuration
SNMP Configuration
Event Configuration
Data Collection & Thresholds: SNMP
MIB Application Builder: SNMP
Load/Unload MIBs: SNMP
Network Polling Configuration: IP/IPX
License Password
Internet
default [Read-Write]
[Auto-Layout] [Connection Labels Off]

The **Event Configuration** window appears. See "Event Configuration and Enterprises window" (page 93).

2 From the list in the **Enterprises** pane, choose the Enterprise trap MIB. In this example, it is **mgmt-traps**.

Copyright © 2007, Nortel Networks

Event Configuration and Enterprises window



Enterprises:

Name	Identifier
dmtfVoltageProbeTable	.1.3.6.1.4.1.412.2.4.53
ENTERPRISES	.1.3.6.1.4.1
entityMIBTraps	.1.3.6.1.2.1.47.2
fmMGCAlarmTraps	.1.3.6.1.4.1.562.3.7.50.4.1
fmSSAlarmTraps	.1.3.6.1.4.1.562.3.21.5.4.1
ManageX	.1.3.6.1.4.1.2427
mgmt-traps	.1.3.6.1.4.1.562.3.10.10.1
OpenView	.1.3.6.1.4.1.11.2.17.1
rmon	.1.3.6.1.2.1.16
snmpTraps	.1.3.6.1.6.3.1.1.5

Events for Enterprise mgmt-traps (.1.3.6.1.4.1.562.3.10.10.1):

Name	Identifier	Sources
commonMIBAlarmCritical	Specific 1	ALL SOURCES
commonMIBAlarmMajor	Specific 2	ALL SOURCES
commonMIBAlarmMinor	Specific 3	ALL SOURCES
commonMIBAlarmWarning	Specific 4	ALL SOURCES
commonMIBAlarmInfo	Specific 5	ALL SOURCES
commonMIBAlarmIndeter…	Specific 6	ALL SOURCES
commonMIBAlarmClear	Specific 7	ALL SOURCES

There are seven possible events that can be configured for the Enterprise example mgmt-traps. For each event, configure the actions to be taken if the event occurs.

3 Choose an event to configure and double-click it.

OR

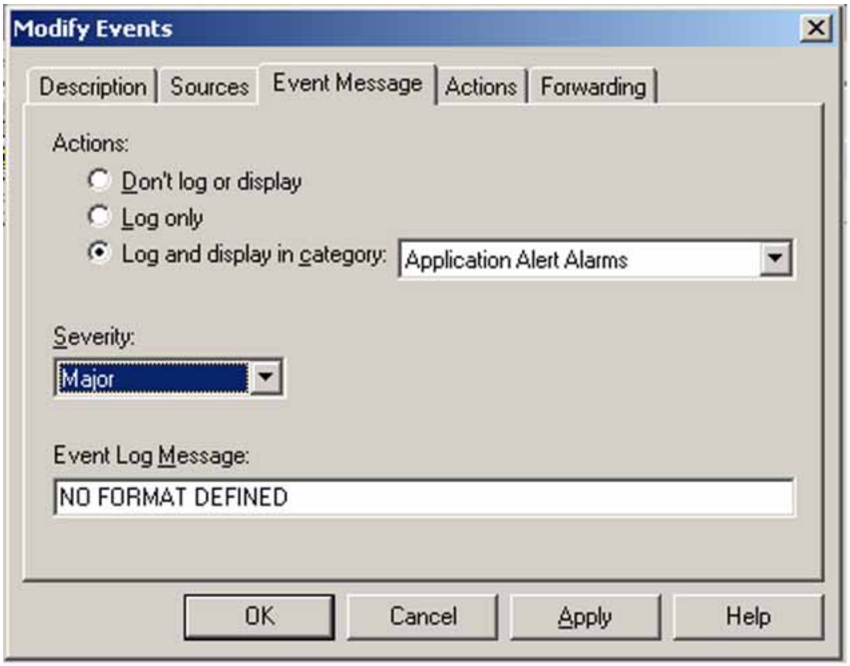
In the upper menu, choose **Edit > Events > Modify**.

The **Modify Events** window appears. See "Modify Events window" (page 94).

4 Configure the event as desired on the various tabs. For example, in the **Event Log Message** text box, shown in "Modify Events window" (page 94), type **$10** to specify that the 10th alarm attribute is to be displayed in the log file. The alarm attribute is the text data of the alarm. Display other attributes by entering the appropriate attribute code.

Copyright © 2007, Nortel Networks

Modify Events window



Actions:

○ Don't log or display

○ Log only

● Log and display in category: Application Alert Alarms

Severity: Major

Event Log Message: NO FORMAT DEFINED

5 Click **Apply**.

The **Modify Events** window closes and the **Event Configuration** window reappears.

6 Repeat steps 3 and 4 for all the events you are configuring.

7 Click **Apply**.

8 In the **File** menu, select **Save**.

9 In the **File** menu, select**Close**.

—End—

Alarm logging and viewing

This section contains details about the Alarm logs and other tools.

Alarm Log

After events are configured, they appear in the Alarm Log.

Copyright © 2007, Nortel Networks

Other tools

You can now configure other tools, such as:

- paging alerts
- e-mail alerts
- event correlation

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Appendix C
Common Trap Structure

Contents

This appendix contains information about the following topics:

Overview

A Common Trap structure ensures that traps from all CS 1000 system devices, including those on Linux, use the same format. A new common trap MIB (**`COMMON-TRAP-MIB.mib`**) is described in detail in the following sections.

Trap severities

The traps have seven severities that each map to a specific trap code. See "SNMPv1 trap PDU fields" (page 59). A trap type defines the severities, for example, **`commonMIBAlarmMajor`** or **`commonMIBAlarmMinor`**. See Appendix "Common Trap MIB" (page 101). The seven severities are

- Critical
- Major
- Minor
- Warning
- Cleared
- Indeterminate
- Info

Copyright © 2007, Nortel Networks

"Severity mapping table" (page 98) compares the severity mapping of the Common Trap structure to the severity mapping previously used by the Call Server, Signaling Server, and Voice Gateway Media Card. In Release 5.0, all CS 1000 devices use the Common Trap severity mapping.

Severity mapping table

Severity (value) in Common Trap structure	Severity in SS and VGMC	Severity in CS
critical (1)	critical (1)	critical (3)
major (2)	major (2)	major (2)
minor (3)	minor (3)	minor (1)
warning (4)	warning (4)	warning (4)
info (5)	None	info (0)
indeterminate (6)	indeterminate (0)	None
cleared (7)	cleared (5)	cleared (5)

Variable bindings

The common trap MIB has a fixed number of variable bindings. Each trap type has the same number and types of variable bindings. For a description of the Common Trap variable bindings mapping, see "Variable binding mapping table" (page 100).

- **commonMIBSeqNumber:**

  contains a unique sequence number for every trap that is sent out. Filtered traps are not assigned a sequence number.

- **commonMIBDateAndTime:**

  contains the date and time in a common format.

- **commonMIBSeverity:**

  represents the severity of the alarm.

- **commonMIBComponentID:**

  contains a string separated by colons that represents the unique system component that raises the trap. This value is generated dynamically by traps received from system elements. The value is unique within each system.

  The format for the string is: `System=systemname:Site=sitename:Component=componentName`

  Values for systemname and sitename are filled in at the consolidation point as configured through EM on the SNMP Configuration page.

Copyright © 2007, Nortel Networks

The componentName is determined based on the original source of the trap. For mapping details for the system element and the component name, see "commonMIBComponentID mapping" (page 99).

commonMIBComponentID mapping

System elements	Component name
Call Server	CS
Signaling Server	SS
Voice Gateway Media Cards (includes MC32S)	VGMC
Media Gateway Controller	MGC
SIP NRS Linux	NRS
EM/BCC Linux	MGMT

- **commonMIBNotificationID:**

  intended to support clears from system elements that are capable of providing unique IDs for generated traps and corresponding clears. If the system does not provide a unique notification ID, this value is set to zero, indicating that clears are not supported by that system. The combination of commonMIBComponentID and commonMIBNotificationID is unique within a system.

- **commonMIBSourceIPAddress:**

  represents the IP address of the system element that generated the trap.

- **commonMIBErrCode:**

  represents specific error codes generated by a system element.

- **commonMIBAlarmType:**

  represents a broad category as described in commonMIBAlarmData.

- **commonMIBProbableCause:**

  represents probable cause for the alarm, and qualifies the type of alarm that appears in the commonMIBAlarmType field.

- **commonMIBAlarmData:**

  a textual description of the trap. Text fields like Alarm Description, Operator Data, and Expert Data are consolidated into a single field . Operator Data is first, Alarm Description second, and Expert Data third, separated by semicolons. This field is truncated if the combined size becomes too large for a single variable binding.

Copyright © 2007, Nortel Networks

"Variable binding mapping table" (page 100) provides a comparison of the variable bindings found in traps in previous releases for the Call Server, Signaling Server, and Voice Gateway Media Card to the new Common Trap format variable bindings.

Variable binding mapping table

Variable binding in Common Trap Structure	Variable binding in SS and VGMC	Variable binding in CS	Variable binding in Linux Trap
commonMIBSeqNumber	None	None	None
commonMIBDateAndTime	EventTime	AlarmTime	commonMIBDateAndTime
commonMIBSeverity	Severity	AlarmSeverity	commonMIBSeverity
commonMIBNotificationID	None	None	commonMIBNotificationID
commonMIBcomponentID	combination of ComponentName and Component OID	combination of ComponentName and Component OID	commonMIBcomponentID
commonMIBSourceIPAddress	IP address of element from trap header	IP address of element from trap header	commonMIBSourceIPAddress
commonMIBErrCode	NTP Index	ErrorCode	commonMIBErrCode
commonMIBAlarmType	AlarmType	Constant value unknown is inserted according to ITU specification	commonMIBAlarmType
commonMIBProbableCause	ProbableCause	Constant value unknown is inserted for all the traps from CS	commonMIBProbableCause
commonMIBAlarmData	OperatorData (or Comment)	OperatorData Description text and ExpertData are combined and values are separated by a colon (:)	commonMIBAlarmData

Copyright © 2007, Nortel Networks

Appendix D
Common Trap MIB

The Common Trap MIB contains definitions of the sysObjectID values for all devices that appear in a MIB-II sysObjectID query. Download the latest version of the MIBs for Nortel products from www.nortel.com.

The Common Trap MIB OID structure for trap and variable bindings are described in the following section:

```
COMMON-TRAP-MIB
--FORCE-INCLUDE <mib.h>
--FORCE-INCLUDE <snmpdefs.h>
--FORCE-INCLUDE <snmpstat.h>
DEFINITIONS ::= BEGIN
-- TITLE: Common Trap MIB
--
-- Author:  Madhukeshwar Hegde
--
-- This specification has been successfully compiled
with the following
-- MIB compilers:
-- a) Wind River Systems Emissary SNMP MIB Compiler,
version 7.0
--
-- Note:
-- This document is maintained as a text file.
IMPORTS
OBJECT-TYPE, MODULE-IDENTITY, enterprises FROM
SNMPv2-SMI DateAndTime FROM SNMPv2-TC
TRAP-TYPE FROM RFC-1215 DisplayString FROM RFC1213-MIB;
commontrapmib MODULE-IDENTITY
LAST-UPDATED "0610261630Z"
ORGANIZATION "Nortel Networks"
CONTACT-INFO
"Postal:  Nortel Networks
250 Sidney Street
```

Copyright © 2007, Nortel Networks

```
Belleville ON K8P 3Z3
Tel :  +1 613 967 5000"
DESCRIPTION
"The common SNMP trap MIB for CS 1000 system."
::= { management 50 }
-- LAST-UPDATED field is in UTC Time Format
-- YYMMDDHHMMZ
-- where:  YY - last two digits of year MM - month (01
through 12)
-- DD - day of month (01 through 31) HH - hours (00
through 23)
-- MM - minutes (00 through 59)
-- Z - the character "Z" denotes Greenwich Mean Time
(GMT).
-- For example, "0302191600Z" represents 4:00pm GMT on
19 February 2003.
nt OBJECT IDENTIFIER ::= { enterprises 562 }
-- nt.  The name under which 562 is registered with
IANA.
meridian OBJECT IDENTIFIER ::= { nt 3 }
-- Meridian.  The value assigned for Meridian.
management OBJECT IDENTIFIER ::= { meridian 10 }
-- management.  The value assigned for management.
fm-info OBJECT IDENTIFIER ::= { management 10 }
-- fm-info.  The value assigned for management
information.
mgmt-traps OBJECT IDENTIFIER ::= { fm-info 1 }
-- mgmt-traps.  The value assigned for management
traps.  mgmt-info OBJECT IDENTIFIER ::= { fm-info 2 }
-- mgmt-info.  The value assigned for management
information.
-- Device definitions
-- defines OIDs associated with different devices
-- Call Server uses the meridian definition
sigserv OBJECT IDENTIFIER ::= { meridian 21 }
-- sigserv The value assigned for Signaling Server
itg OBJECT IDENTIFIER ::= { meridian 11 }
-- itg.  The value assigned for ITG.
iplmib OBJECT IDENTIFIER ::= { itg 5 }
-- iplmib.  The value assigned for VGMC cards
mgc OBJECT IDENTIFIER ::= { meridian 7 }
-- mgc.  The value assigned for Media Gateway
Controller.
nrs OBJECT IDENTIFIER ::= { meridian 12 }
-- nrs.  The value assigned for NRS (on Linux).
ecm OBJECT IDENTIFIER ::= { meridian 13 }
```

Copyright © 2007, Nortel Networks

```
-- ecm.  The value assigned for ECM management(on
Linux).
-- General definitions
AlarmSeverity ::= INTEGER { critical (1),
major (2),
minor (3),
warning (4),
info (5),
indeterminate(6),
cleared (7)
}
AlarmType ::= INTEGER {
communications(1),
qualityOfService(2),
processing(3),
equipment(4),
security(5),
operator(6),
debug(7),
unknown(8)
}
-- Fault management alarm types
commonMIBAlarmCritical TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication of
a critical alarm condition.  The variables listed in
VARIABLES clause are defined in ‘mgmt-info’group and
are present in all critical alarms."
::= 1
commonMIBAlarmMajor TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
```

Copyright © 2007, Nortel Networks

```
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication
of a Major alarm condition.  The variables listed in
VARIABLES clause are defined in ‘mgmt-info’ group and
are present in all major alarms."
::= 2
commonMIBAlarmMinor TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication
of a Minor alarm condition.  The variables listed in
VARIABLES clause are defined in ‘mgmt-info’ group and
are present in all minor alarms."
::= 3
commonMIBAlarmWarning TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
```

Copyright © 2007, Nortel Networks

```
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication
of a Warning alarm condition.  The variables listed in
VARIABLES clause are defined in ‘mgmt-info’ group and
are present in all warning alarms."
::= 4
commonMIBAlarmInfo TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication of
an informational alarm condition.  The variables listed
in VARIABLES clause are defined in ‘mgmt-info’ group
and are present in all info alarms."
::= 5
commonMIBAlarmIndeterminate TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication of
an indeterminate alarm condition.  The variables listed
in VARIABLES clause are defined in ‘mgmt-info’ group
and are present in all indeterminate alarms."
```

Copyright © 2007, Nortel Networks

```
::= 6
commonMIBAlarmClear TRAP-TYPE
ENTERPRISE mgmt-traps
VARIABLES {
commonMIBSeqNumber,
commonMIBDateAndTime,
commonMIBSeverity,
commonMIBComponentID,
commonMIBNotificationID,
commonMIBSourceIPAddress,
commonMIBErrCode,
commonMIBAlarmType,
commonMIBProbableCause,
commonMIBAlarmData
}
DESCRIPTION
"This trap is used to provide a real time indication
of a clear alarm condition.  The variables listed in
VARIABLES clause are defined in ‘mgmt-info’ group and
are present in all clear alarms."
::= 7
commonMIBSeqNumber OBJECT-TYPE
SYNTAX INTEGER (9999)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Sequence number of the alarm; starts at 1 and
increments by 1;
must be unique for all alarms emitted from commonMIB."
::= { mgmt-info 1 }
commonMIBDateAndTime OBJECT-TYPE
SYNTAX DateAndTime
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Time at which the alarm occurred."
::= { mgmt-info 2 }
commonMIBSeverity OBJECT-TYPE
SYNTAX AlarmSeverity
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The severity of the alarm which should indicate the
priority of the event"
::= { mgmt-info 3 }
commonMIBComponentID OBJECT-TYPE
SYNTAX DisplayString (SIZE(264))
```

Copyright © 2007, Nortel Networks

```
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This variable binding contains colon (:)  separated
string uniquely representing the system component
that raised this trap.  This varbind is in '<system-
Name>:<siteName>:<componentName>'format.  This is
generated dynamically from traps received from system
elements and for each element it would be unique within
system"
::= { mgmt-info 4 }
commonMIBNotificationID OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This variable binding is intended to support clears
from system elements that are capable of providing
unique Id for generated traps and their corresponding
clears.  If system element does not provide unique
notification id, this value would be set to 0
indicating that system do not support clears.   "
::= { mgmt-info 5 }
commonMIBSourceIPAddress OBJECT-TYPE
SYNTAX DisplayString (SIZE(7..23))-- NetworkAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The IP address of the element that originated the
trap."
::= { mgmt-info 6 }
commonMIBErrCode OBJECT-TYPE
SYNTAX DisplayString(SIZE(8))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Represents specific error code generated by any system
element."
::= { mgmt-info 7}
commonMIBAlarmType OBJECT-TYPE
SYNTAX AlarmType
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The alarm type field as defined by OSI which is
used to indicate a broad category of what is wrong.
The first 6 values are OSI-defined; refer to CCITT
```

Copyright © 2007, Nortel Networks

```
X.733/ISO 10164-4 (for the first 5) and CCITT X.736/ISO
10164-4 (for the last) for a more complete description.
The value 'operator' is used when an alarm is issued
due to an operator command.  The values 'debug' and
'unknown' are for compatibility with older switches and
are used for debugging alarms and for those which do
not fit any of the above, respectively."
::= { mgmt-info 8}
commonMIBProbableCause OBJECT-TYPE
SYNTAX INTEGER {
-- Start of OSI-defined values
-- (see X.733/ ISO 10165-3)
lossOfSignal(0),
lossOfFrame(1),
framingError(2),
localTransmissionError(3),
remoteTransmissionError(4),
callEstablishmentError(5),
degradedSignal(6),
commSubsystemFailure(7),
commProtocolError(8),
lanError(9),
dteDceInterfaceError(10),
responseTimeExcessive(20),
queueSizeExceeded(21),
bandwidthReduced(22),
retransmissionRateReduced(23),
thresholdCrossed(24),
performanceDegraded(25),
congestion(26),
atOrNearCapacity(27),
storageCapacityProblem(40),
versionMismatch(41),
corruptData(42),
cpuCyclesLimitExceeded(43),
softwareError(44),
softwareProgramError(45),
softwareProgramTermination(46),
fileError(47),
outOfMemory(48),
underlyingResourceUnavail(49),
applicationSubsystemFailure(50),
configurationError(51),
powerProblem(60),
timingProblem(61),
processorProblem(62),
datasetModemError(63),
```

Copyright © 2007, Nortel Networks

```
multiplexorProblem(64),
receiverFailure(65),
transmitterFailure(66),
outputDeviceError(67),
inputDeviceError(68),
ioDeviceError(69),
equipmentFailure(70),
adapterError(71),
-- OSI-defined values continued (see X.736)
duplicateInfo(80),
infoMissing(81),
infoModification(82),
infoOutOfSequence(83),
unexpectedInfo(84),
denialOfService(90),
outOfService(91),
proceduralError(92),
otherOperational(93),
cableTamper(100),
intrusionDetection(101),
otherPhysical(102),
authenticationFailure(110),
breachOfConfidence(111),
nonRepudiationFailure(112),
unauthorizedMAX-ACCESS(113),
otherSecurityService(114),
delayedInfo(120),
keyExpired(121),
outOfHoursActivity(122),
-- Start of non-OSI defined values
operationalCondition(200),
debugging(201),
unknown(202),
inactiveVirtualCircuit(203),
networkServerIntervention(204)
}
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The probable cause for the alarm which usually
qualifies the Alarm Type field.  Most values are
OSI-defined; refer to CCITT X.733 and X.736 (ISO
10164-4 and 10164-7) for a more complete description."
::= { mgmt-info 9 }
commonMIBAlarmData OBJECT-TYPE
SYNTAX DisplayString ( SIZE (0..750) )
MAX-ACCESS read-only
```

Copyright © 2007, Nortel Networks

```
STATUS current
DESCRIPTION
"This variable binding represents textual description
of trap."
::= { mgmt-info 10}
END
```

Copyright © 2007, Nortel Networks

List of terms

BUG

A system message category associated with the Software Error Monitor, which is a program that continuously monitors call processing. When invalid information is detected, a BUG message is printed.

EDT

Event Default Table. Table of default event entries and associated severities.

EPT

Event Preference Table. Table of customer's event entries with associated severities.

ERR

Error (Hardware). A system message category associated with the Software Error Monitor, which is a program that continuously monitors call processing. When information is detected that is not in the correct format or invalid, an ERR message is printed.

ITG

Integrated IP Telephony Gateway. A system message category associated with the Integrated IP Telephony Gateway component, which generates a trap message from the Voice Media Gateway Card and Signaling Server. The trap message incorporates the severity category of the message in the first digit of the four-digit number.

ITS

Integrated IP Telephony Server. A system message category associated with the Integrated IP Telephony Server component which generates a trap message from the Internet Telephone and reports it through the Signaling Server. ITS trap messages incorporate the severity category of the message in the first-digit of the four digit number.

Copyright © 2007, Nortel Networks

QoS

Quality of Service. Uses Proactive Voice Quality (PVQ) monitoring to assist crafts persons to diagnose, isolate, and correct networking issues that cause deterioration of voice quality. QoS can also refer to a system message category for traps issued for Quality of Service events.

SELSIZE

System Event List Size. The number of events in System Event Log.

SEL

System Event List. A list of system events that are viewed in a log file.

SUPPRESS

Suppress count. The number of times the same event is processed before it is suppressed.

TIMER

Global window timer length.

WEB

Web Server. A system message category associated with the Software Error Monitor, which generates a trap message between the CS 1000 Web server, Remote Procedure Call (RPC) Server, and Call Server.

Copyright © 2007, Nortel Networks

Index

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Copyright © 2007, Nortel Networks

Nortel Communication Server 1000

Communication Server 1000 Fault Management — SNMP

Copyright © 2007, Nortel Networks
All Rights Reserved.

Publication: NN43001-719
Document status: Standard
Document version: 02.02
Document date: 7 December 2007

To provide feedback or report a problem in the document, go to www.nortel.com/documentfeedback.

Sourced in Canada

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.
All other trademarks are the property of their respective owners.