Fault Management — SNMP
Avaya Communication Server 1000

7.5
NN43001-719, 05.02
November 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release

The following sections detail what's new in *Avaya Communication Server 1000 Fault Management — SNMP, NN43001-719* for Avaya Communications Server 1000 Release 7.5.

Features

There are no updates to the feature descriptions in this document.

SNMP Profile Manager for High Scalability systems

SNMP Profile Manager for High Scalability systems allows you to view all elements registered to the UCM security domain in a tree view. You can select up to 500 individual or multiple elements for system-wide profile management and distribution.

Other changes

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

Revision history

November 2010	Standard 05.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
June 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.

May 2009	Standard 03.02. This document is up-issued to include changes to technical content.
May 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0. This document may contain information on or refer to products and naming conventions that are not supported in this release. This information is included for legacy purposes and convenience only. This includes but is not limited to items, such as: SSC; ISP 1100; ITG Pentium cards; and Media Cards running certain IP Line applications.
February 2008	Standard 02.03. This document is up-issued to include new and altered SNMP CLI commands.
December 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 (Supported MIBs on page 79) and a list of space utilization thresholds (Supported MIBs on page 79).
December 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.
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 Confidential statement.
May 2007	Standard 01.01. This document is issued to support 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 on page 45 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 on page 45 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 and Signaling Server, Voice Gateway media Card, and MGC default community strings. 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.
August 2005	Standard 2.00. This document is up-issued to support Communication Server 1000 Release 4.5.
September 2004	Standard 1.00. This document is issued to support Simple Network Management Protocol (SNMP) capabilities for Communication Server 1000 Release 4.0 and Meridian 1 systems.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

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

Important:

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 Avaya Communication 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), Gateway Controller, Network Routing Service (NRS), and Unified Communications Management (UCM). It describes how SNMP is configured, and how it operates to allow the management system to receive management information about the system components.

For information about SNMP capabilities for Survivable Remote Gateway (SRG), see *Avaya Survivable Remote Gateway Configuration Guide, NN42120-501*.

Legacy products and releases

This document contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 software. For more information about legacy products and releases, click the Documentation link under Support on the Avaya home page: www.avaya.com.

Applicable systems

This document applies to the following systems:

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

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

- *Avaya Communication Server 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*
- *Avaya 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 Avaya systems are referred to generically as system:

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

In this document, the following circuit cards are referred to generically as Gateway Controller:

- Media Gateway Controller (MGC) card
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card
- Common Processor Media Gateway (CP MG) card

In this document, the information for MGC applies to all Avaya Gateway Controller platforms unless otherwise specified.

In this document, the following hardware platforms are referred to generically as Server.

- Call Processor Pentium IV (CP PIV)
- Common Processor Pentium Mobile (CP PM)
- Common Processor Media Gateway (CP MG)
- Common Processor Dual Core (CP DC)
- Commercial off-the-shelf (COTS) servers
    - IBM x306m server (COTS1)
    - IBM DL320 G4 server (COTS1)
    - IBM x3350 server (COTS2)
    - Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

Related information

This section lists information sources that relate to this document.

Documentation

The following technical publications are referenced in this document:

- *Avaya Network Routing Service Fundamentals, NN43001-130*
- *Converging the Avaya Data Network with VoIP, NN43001-260*
- *Avaya IP Peer Networking Installation and Commissioning, NN43001-313*
- *Avaya IP Trunk Description, Installation, and Operation, NN43001-563*
- *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Avaya Software Input/Output System Messages, NN43001-712*
- *Avaya Software Input/Output Maintenance, NN43001-711*
- *Avaya Communication Server 1000M and Meridian 1 Small System Maintenance, NN43011-700*
- *Avaya Communication Server 1000M and Meridian 1 Large System Maintenance, NN43021-700*

- *Avaya Communication Server 1000E Maintenance, NN43041-700*
- *Installing Avaya Enterprise Network Management System, 321537-B*
- *Administering Avaya Enterprise Network Management System, 205969-J*
- *Using Avaya Enterprise Network Management System, 207569-G*

Online

To access Avaya documentation online, click the Documentation link under Support on the Avaya home page: www.avaya.com

Chapter 4: 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.

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.

Profile – a logical group of SNMP parameters configured and assigned to UCM-managed network elements.

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 *Avaya 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 Avaya Communication Server 1000 products, the traps are sent in the form of a 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 a 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.

`getRequest` command – a 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 Figure 1: Management system responsibilities on page 20.

  When the request is received, the agent on the device returns the requested data. See Figure 2: Agent responsibilities on page 20.

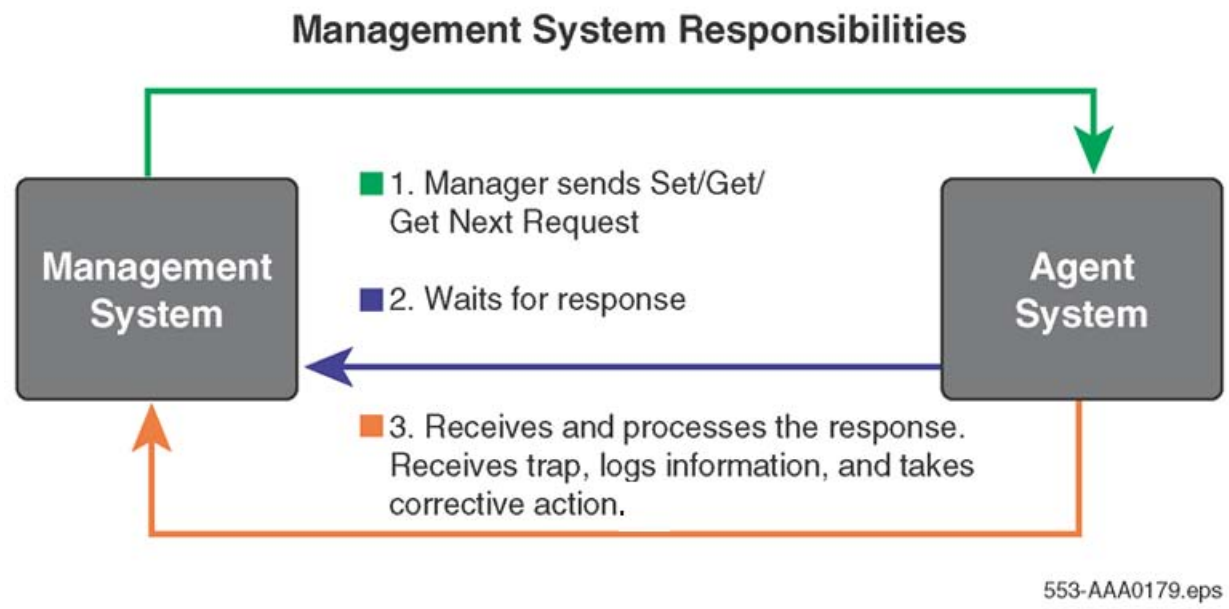


Figure 1: Management system responsibilities

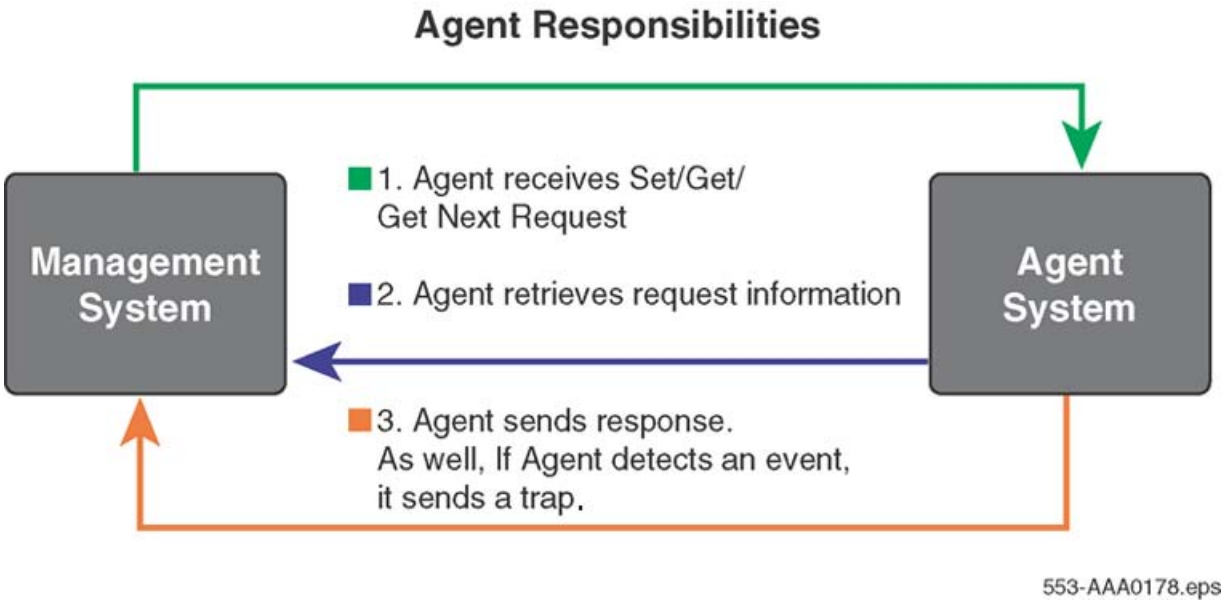


Figure 2: Agent responsibilities

You can perform fault management configuration at the network level or at the system level. At the network level the SNMP Profile configuration interface, the UCM SNMP Profile Manager, is hosted on the UCM Primary security server. This element must be active for the network level configuration to be available as the capability is not available on the UCM Backup security server or on any other element.

System level configuration is performed using the Element Manager for the system or by the CLI interface of the Avaya Communication Server 1000 Call Server.

SNMP capabilities

To understand how SNMP operates on a system running Avaya Communication Server 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
- Gateway Controllers
- Voice Gateway Media Cards
- Network Routing Service (NRS)
- Unified Communications Management (UCM)

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 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 Glossary for a description of the trap message types.

Note:
Elements on Linux platforms (such as Co-resident Call Server and Signaling Server, NRS, Signaling Server, Management System) support UCD-SNMP-MIB, which has the same access privileges as MIB-II. Call Servers with VxWorks platforms do not support UCD-SNMP MIB.

Logical architecture of fault management

Fault management is implemented in Element Manager and hosted on the Unified Communications Management (UCM) Common Services framework. UCM provides a generic launch point, a common user interface, and a generic infrastructure for all applications. UCM is installed on a Linux operating system and Java is the technology used for fault management implementation.

SNMP profiles

Logical groups of SNMP parameters are called SNMP profiles. There are three types of SNMP profiles: MIB Access, System Info, and Alarm.

Table 1: SNMP profile names and descriptions

Profile name	Description
MIBACCESS	This profile contains the following items: • Administrator Group1 community string • Administrator Group2 community string • Administrator Group3 community string • System Management Read community string • System Management Write community string
SYSINFO	This profile contains the following items: • System Name—value assigned to MIBII sysName object • System Contact—value assigned to MIBII sysContact object • System Location—value assigned to MIBII sysLocation object • Navigation Site Name—value sent as part of commonMIBComponentID object of common trap • Navigation System Name—value sent as part of commonMIBComponentID object of common trap The System Name has a default default value of %hostname%. If the System Name is configured as %hostname%, this value is replaced with the actual host name of the system when the SNMP GET query occurs on the MIBII System name. For example, an EM system has a host name of EM-HOST, the Call Server has a host name of CS-HOST, and the Signaling Server has a host name of SS-HOST. If a System Info profile with a System Name value of %hostname% is assigned to the EM server and the Call Server and the same profile propagates to the Signaling Server through the Call Server, when the SNMP GET query occurs on the

Profile name	Description
	MIB II System Name on the EM server, the Call Server, and the Signaling Server, the returned values are EM-HOST, CS-HOST, and SS-HOST, respectively.
ALARM	This profile contains the following items: • trap community • alarm Threshold • option to enable or disable trap • eight trap destinations with port numbers **Note:** If you configure the trap destination IP address without specifying a port, the SNMP trap is sent to the default port of the configured destination (port 162).

Note:
If you configure SNMP parameters using overlay 117 or EM, a custom profile is created in SNMP Profile Manager and assigned to the element on which the SNMP parameters are configured. The custom profile is read-only; you cannot modify it using the SNMP Profile Manager.

SNMP Profile Manager

The SNMP Profile Manager runs on the UCM Primary Security Server. It performs SNMP configuration at the security domain level. You can add, modify, and delete SNMP profiles using the SNMP Profile Manager. You can configure and assign profiles to the following types of UCM managed elements:

- Avaya Communication Server 1000 Call Servers

  The configuration settings applied to the Call Server are propagated to all system elements associated with the Call Server, such as Signaling Servers, VGMCs, and Gateway Controllers. These elements are all running CS 1000 applications, such as SIP Line.

- Linux elements running UCM Common Services, but not running Avaya Communication Server 1000 applications

  Examples of these types of elements are standalone NRS elements, the UCM Primary Security Server, or an element running Element Manager, where in all cases there are no other CS 1000 applications installed (such as SIP Line, Signaling Server applications, and so on).

You can add only one profile at a time, but you can delete multiple profiles at one time. A newly added profile is assigned version 1.0. When you update or modify the profile, the version number of the profile increments by one.

SNMP configuration propagation

The SNMP configuration is performed using the SNMP Profiles interface in UCM. This interface is active on the UCM Primary security server and transfers the configuration settings to all the elements. For a Call Server system, the configuration is transferred to the Call Server which then transfers the settings to all system elements.Figure 3: System propagation of SNMP parameters on page 24 shows how the SNMP configuration changes propagate throughout the system.

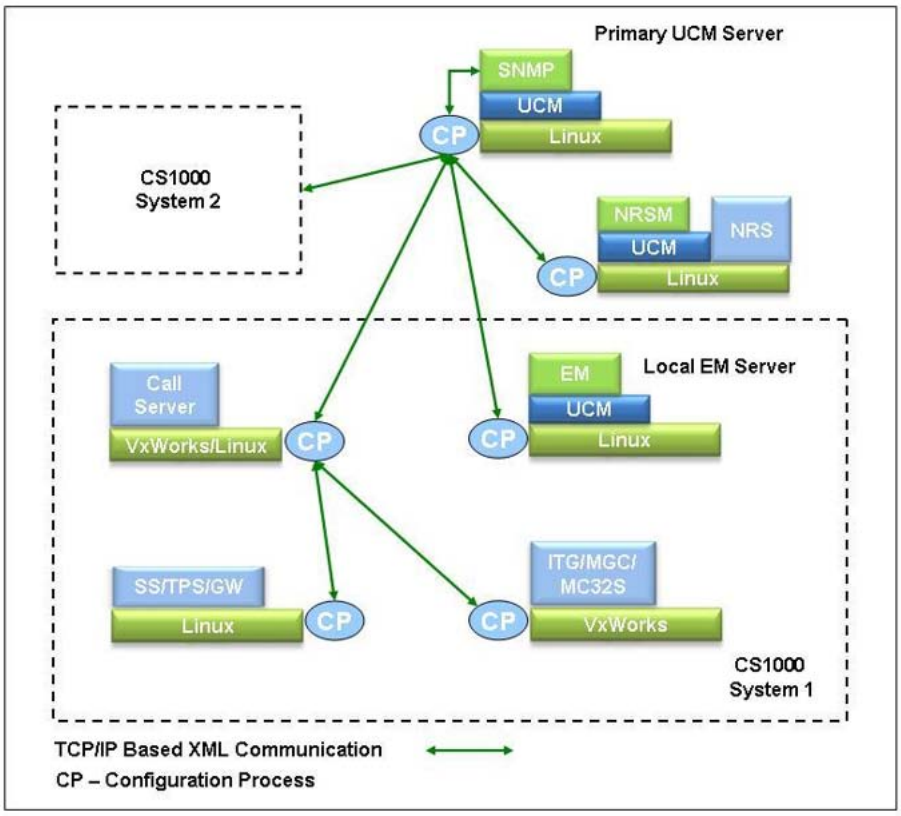


Figure 3: System propagation of SNMP parameters

For SNMP Profile Manager procedures, see SNMP configuration using SNMP Profile Manager on page 53.

System SNMP architecture

There are different architectural models for the Call Server, VxWorks elements, and Linux elements. 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 Figure 4: Event architecture on the Call Server on page 25.

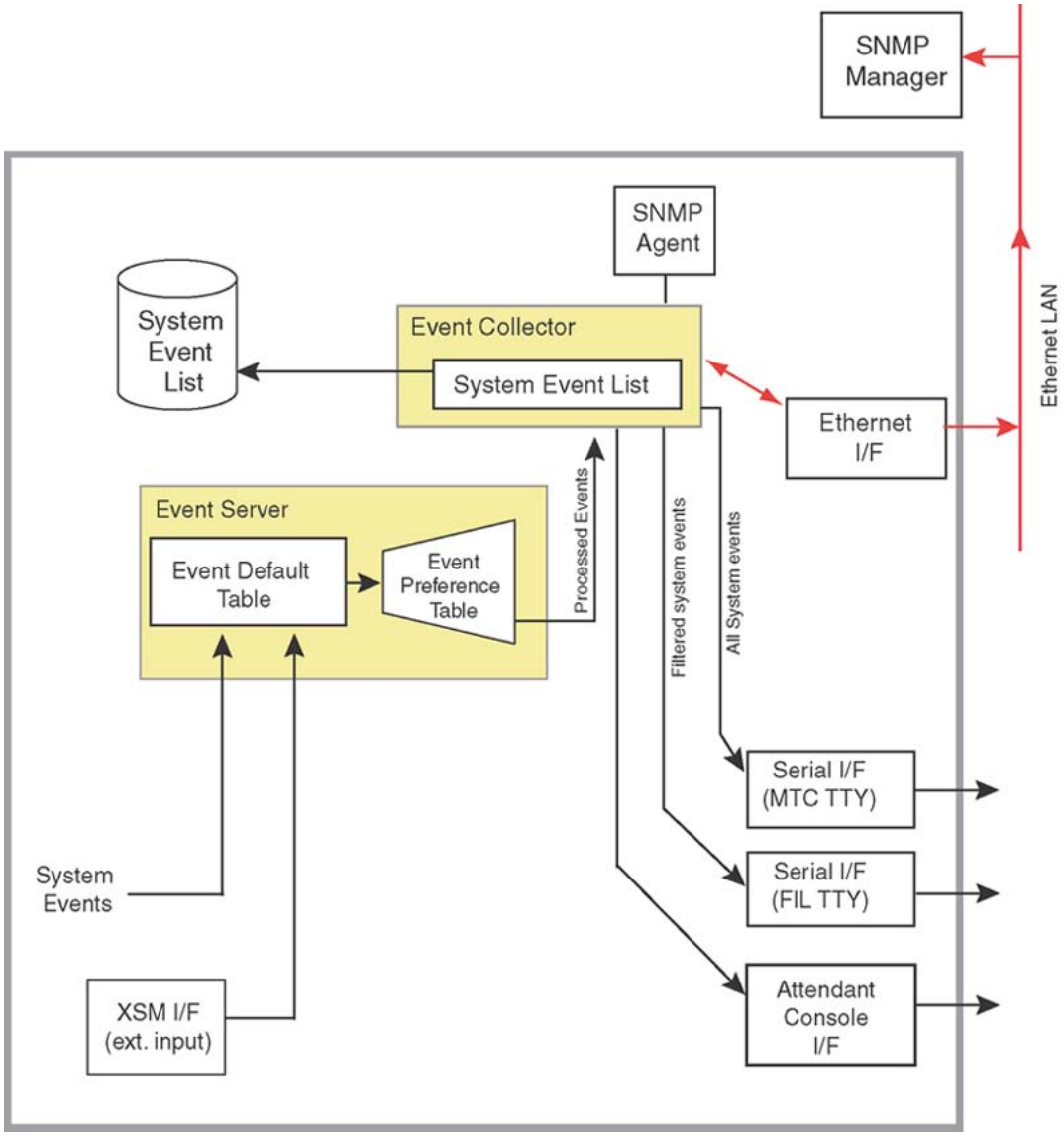


Figure 4: Event architecture on the Call Server

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)

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 Avaya Communication Server 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 *Avaya Software Input/Output System Messages, NN43001-712*.

More information

For more information about the configuration of the Event Server and the Event Collector, see Event Collector on page 41 and Event Server on page 42.

For more information about overriding severities in the EDT, see How to change Event Default Table settings on page 44.

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.

Voice Gateway Media Card and Gateway Controller architecture

The Voice Gateway Media Card and Gateway Controller architectures are similar and consist of the Alarm/SNMP Services, Report Log, and SNMP agent. See Figure 5: Event architecture on the Voice Gateway Media Card and Gateway Controller on page 28.

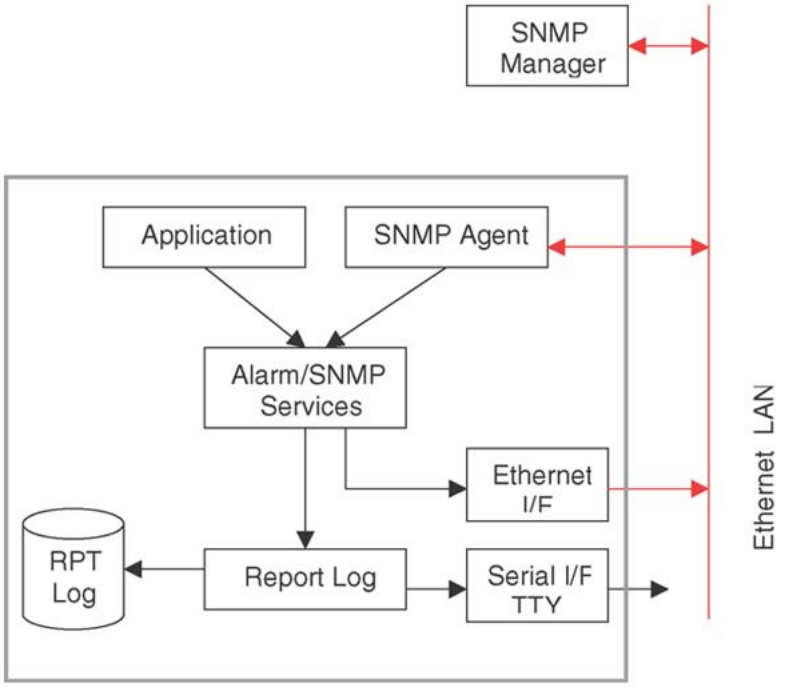


Figure 5: Event architecture on the Voice Gateway Media Card and Gateway Controller

Table 2: Trap generation process on page 28 describes the process of generating a SNMP trap on the Voice Gateway Media Card and Gateway Controller.

Table 2: Trap generation process

Step	Description
1	The application 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 a 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 SNMP architecture

The SNMP architecture on Linux is shown inFigure 6: Common Trap Server in Linux on page 29 and is described in the following sections.

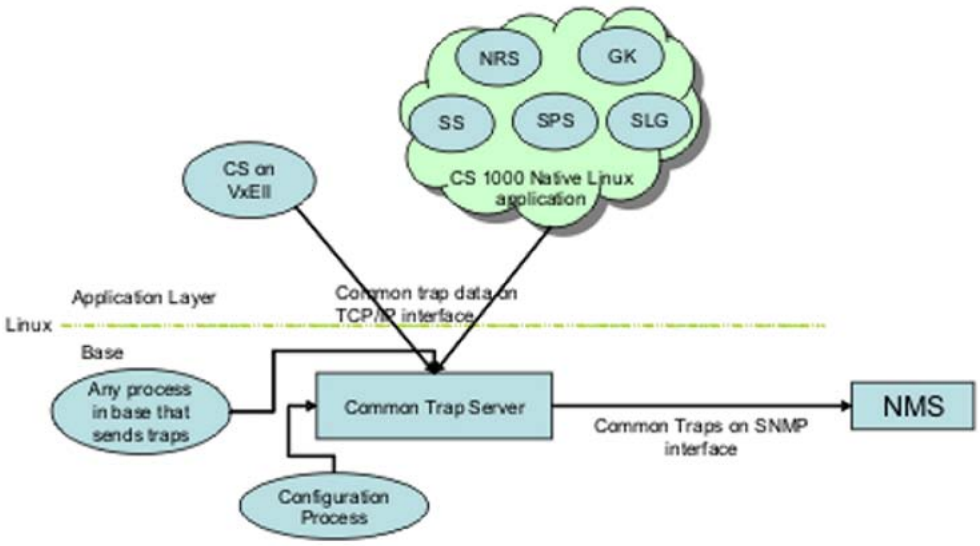


Figure 6: Common Trap Server in Linux

Common Trap Server

Common Trap Server is active in Linux base and binds itself to a predefined TCP/IP port, listening for alarm data sent from any application residing in the same system. On receiving the alarm data from the client applications, it checks for the trap enable/disable flag.

If the trap is enabled, it suppresses the alarm based on the configured severity level. The suppressed alarms are assigned a unique sequence number, navigation site/system name, date and time, source IP address, and community string.

After assigning the above values, the raw alarm data is converted into the trap structure defined by the Common Trap MIB. Generated traps are then forwarded to the configured destinations.

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. Other proprietary MIBs are also supported by the Net-SNMP agent, such as the QOSTRAFFIC-MIB.mib.

Media Application Server SNMP architecture

Media Application Servers (MAS) can be deployed in a system to provide media services, as shown in Figure 7: IP Media Services system architecture on page 30. Media Application Servers run on Linux base and send SNMP traps using the Avaya Reliability MIB, as opposed to the Common Trap MIB used by other Avaya Communication Server 1000 applications.

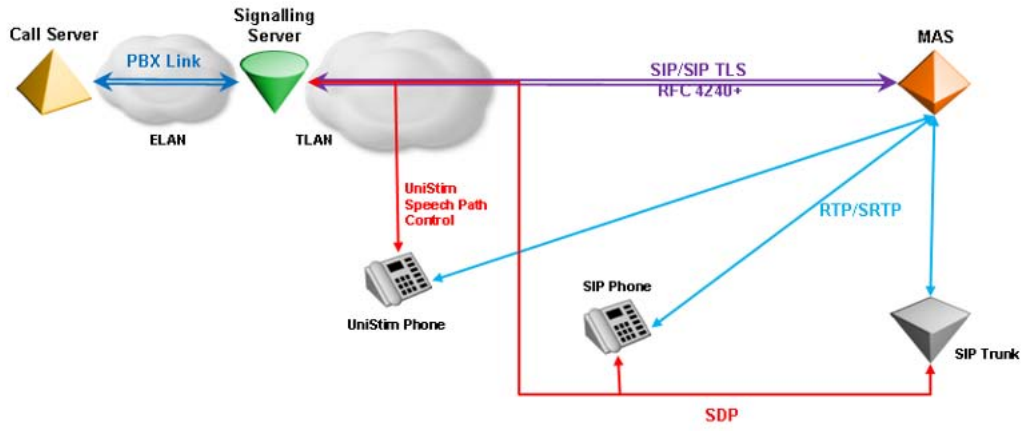


Figure 7: IP Media Services system architecture

Network management systems receiving SNMP traps from MAS elements receive both Avaya Reliability MIB (MAS) and Common Trap MIB (Communication Server 1000) formats. MAS

only sends outgoing SNMP traps. There is no support for SNMP queries relating to the Avaya Reliability MIB.

Note:

MAS only supports a single trap destination, unlike Communication Server 1000 Common MIB traps that support up to eight destinations.

Configuration of the SNMP trap destination for MAS must be performed separately using the MAS management interface. For information about MIBs for MAS, refer to the MAS documentation.

Connections

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

Access to SNMP components

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

Avaya 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 *Avaya Software Input/Output System Messages, NN43001-712*.

For information about trap components, see Trap format on page 66.

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

Most elements have both ELAN and TLAN network interface connections. However, the Call Server will only have an ELAN network interface if it does not have co-resident Signaling Server applications. 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 all elements. Each trap destination IP address is verified whether it

belongs to same ELAN/TLAN subnet or not. If a trap destination IP address does not belong to the same ELAN/TLAN subnet, it is added to the network routing table with the ELAN gateway as its gateway. If the trap destination configurations are removed, the matching entry is removed from the network routing table.

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 *Avaya Element Manager System Administration, NN43001-632*.

The MGC has an Element Manager interface to add routing entries.

Trap and MIB access

SNMP traps are sent out using the ELAN interface. Table 3: MIB access by interface on page 32 lists various elements and their MIB access by ELAN and TLAN interface. These properties apply to all MIBs supported on each respective element.

Table 3: MIB access by interface

Element	ELAN	TLAN
Co-resident Call Server and Signaling Server (Linux)	YES	YES
Call Server (CP PIV)	YES	N/A
Call Server (CP PM)	YES	N/A
COTS (Linux)	YES	YES
Gateway Controller	YES	NO
MC32S	YES	NO
ITG-SA	YES	NO

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 Figure 8: Typical SNMP Ethernet LAN on page 33.

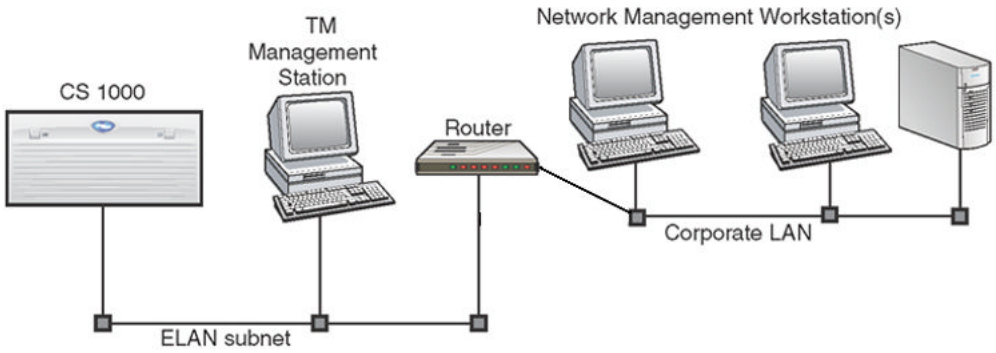


Figure 8: Typical SNMP Ethernet LAN

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.

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 Figure 9: Typical SNMP Ethernet WAN on page 33.

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

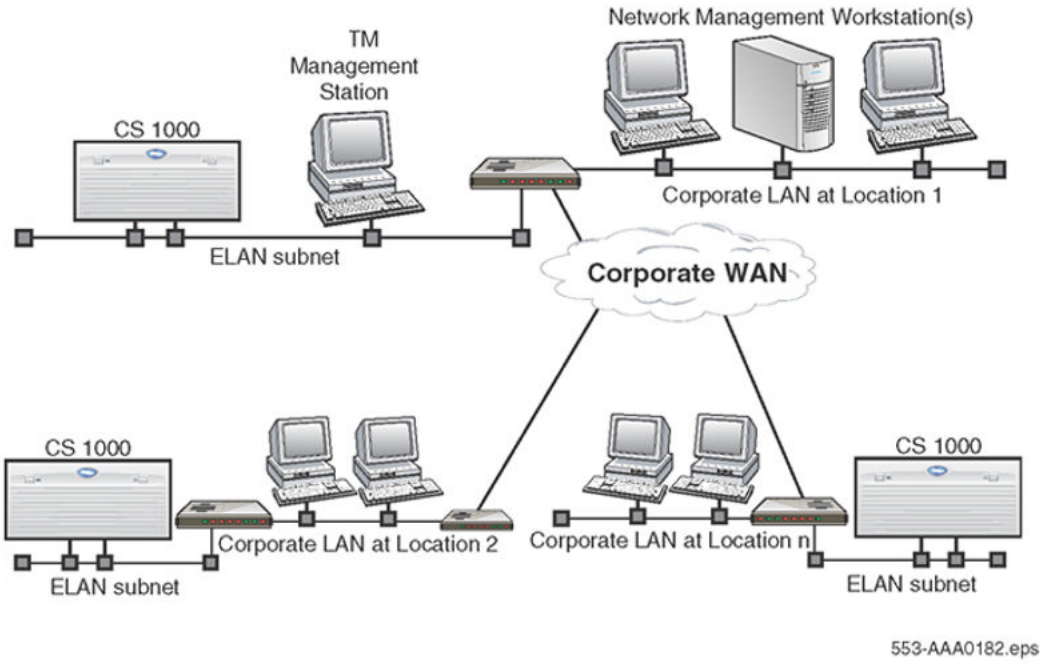


Figure 9: Typical SNMP Ethernet WAN

Call Server and IP Telephony device connections

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

Geographic Redundancy SNMP configuration

For systems configured with Geographic Redundancy, SNMP configuration data from the Primary Call Server is not synchronized with the Secondary Call Servers. You can use SNMP Profile Manager to configure and assign SNMP profiles to multiple elements, or you can perform SNMP configuration separately on each Secondary Call Server using either CLI (LD 117) or Element Manager.

SNMP and ISSS/IPsec

SNMP configuration information cannot be passed between SNMP Profile Manager and a Avaya Communication Server 1000 Call Server when IPsec is configured with an Intra System Signaling Security (ISSS) level of Full.

However, there is an exception to this if the UCM Primary Security Server resides on an element associated with the system, because then it is included in the UCM security domain. In this case, the UCM Primary Security Server has a system application, such as Call Server, Signaling Server applications, or SIP Line application running on the same element. Configuration by SNMP Profile Manager for this system will function correctly with an ISSS level of Full because IPsec communication is enabled between all system elements.

If you use an ISSS level of Full for a system, Avaya recommends that you perform SNMP configuration using Element Manager or the CLI (LD 117). All system elements will be correctly configured. SNMP Profile Manager is normally notified of configuration changes, such as a custom profile being used for that system. However, in this case, there is no communication possible with the SNMP Profile Manager. As a result, the SNMP Profile Manager cannot accurately reflect the configuration status of the system, and such information should be ignored.

There may be cases where a lower level of ISSS is initially used on a system (None or Optimal). If SNMP Profile Manager is used to configure SNMP for a system, such functionality will cease to work after ISSS is set to Full. You can then use Element Manager or CLI (LD 117) to modify SNMP configuration, thereby converting to custom SNMP profiles.

For more information about ISSS/IPsec, see *Avaya Security Management Fundamentals, NN43001-604*.

Chapter 5: Configuring SNMP

Contents

This chapter contains Information about the following topics:

Overview

You can use various methods (UCM SNMP Profile Manager, Command Line Interface [CLI], or Element Manager) to configure SNMP for a system, depending on the system platform (Avaya Communication Server 1000 or Meridian 1) and the network device.

Note:

SNMP Profile Manager only manages Linux elements that are registered with the UCM Primary Security Server and are thus members of the same security domain. If an element does not have an established PBXLink with a Call Server, you cannot configure it using Element Manager or the Call Server CLI. For an element that is outside of the UCM security domain, you can choose not to support SNMP on the element, which means that it will not send SNMP traps or respond to MIB queries. Or, if SNMP support is desired for the element, you can configure it as a standalone UCM Primary Security Server within its own security domain. This option allows you to use SNMP Profile Manager to configure SNMP for the

element, but it is not recognized as a trusted member by elements within other UCM security domains.

SNMP configuration entails configuring the following components:

- trap destinations
- community strings (to access MIBs)
- trap community
- Call Server filtering (EDT, EPT, and alarm suppression thresholds)
- MIB II system group values

Table 4: Interfaces for configuring SNMP on page 38 describes where you configure the various elements.

Table 4: Interfaces for configuring SNMP

SNMP configuration of	Call Server CLI	Element Manager	SNMP Profile Manager
Admin group community strings	Yes	Yes	Yes
Trap community string	Yes	Yes	Yes
Trap destinations	Yes	Yes	Yes
MIB II system group values	Yes	Yes	Yes
EDT/EPT edits	Yes	Yes	No
Alarm suppression threshold edits	Yes	Yes	Yes

Note:
The configuration propagates to all system elements (Voice Gateway Media Cards, Media Gateway Controllers, Signaling Servers) when you issue the **`sync snmpconf`** command.

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 Voice Gateway Media Card and Gateway Controller 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.

When you use LD 117 commands to perform SNMP configuration, the changes do not automatically propagate throughout the system. You must run the SYNC SNMPCONF command to propagate the configured SNMP parameters to the Call Server and all network elements with an established PBXlink to the Call Server, such as Signaling Server, VGMC, or Gateway Controller.

In addition, changes to SNMP parameters are noted by the SNMP Profile Manager in UCM, which creates a custom profile. A custom profile is created whenever you configure SNMP parameters using LD 117 or the SNMP configuration pages in Element Manager.

Note:
If a Call Server already has an assigned profile from the SNMP Profile Manager, that profile is replaced with the custom profile. No warning message appears when a preassigned profile is replaced with a custom profile.

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.

- 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.

Important:
If you make changes to the EDT/EPT parameters, a data dump (EDD) must be performed.

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 Gateway Controllers.

For the command syntax, see Table 10: Commands - alphabetical order on page 46.

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 on page 40.

Verifying the SNMP configuration

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
   - 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.

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 a 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 Table 10: Commands - alphabetical order on page 46 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.

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. Table 5: Sample Event Default Table entries on page 42 lists examples of Event defaults.

   Table 5: 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 Table 6: Sample Event Preference Table (EPT) on page 42.

Table 6: 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:
The question mark (?) is a wildcard. See Wildcards on page 43 for an explanation of wildcard entries.

Error Code	Severity	Escalate Threshold (events/60 sec.) (see Note 2)

Note:
The window timer length defaults to 60 seconds, however, the administrator can change this value. See Global window timer length on page 43 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 by 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.

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 Table 10: Commands - alphabetical order on page 46.

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.

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 on page 43 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. Configure and view community strings using the interface from which the device was originally configured.

Use commands in LD 117 to configure MIB community strings for access to Call Server MIBs (MIB-II objects), Voice Gateway Media Card, Signaling Server, and Gateway Controller MIBs.Table 7: MIB access by community string on page 45 lists the MIB access for community strings, Table 8: MIB access by system element on page 45lists MIB access by system element or platform, and Table 9: Trap community string on page 46lists the system management trap community string that applies to all system elements.

Table 7: MIB access by community string

Community String	MIB			
	MIB-II	Entity-MIB	QOSTRAFFIC-MIB	QOS.MIB
ADMIN_COMM1 (admingroup1)	READ	READ	N/A	N/A
ADMIN_COMM2 (admingroup2)	READ	READ	READ	READ
ADMIN_COMM3 (admingroup3)	READ	READ	N/A	N/A
SYSMGMT_RD_COMM (otm123)	READ	READ	READ	READ
SYSMGMT_WR_COMM (otm321)	READ	READ	READ	READ

Table 8: MIB access by system element

Element	MIB			
	MIB-II	Entity-MIB	QOSTRAFFIC-MIB	QOS-MIB
Call Server	YES	YES	YES	NO
Co-resident Call Server and Signaling Server	YES	YES	YES	YES
Signaling Server	YES	NO	NO	YES
Gateway Controller	YES	NO	NO	NO

MC32S	YES	NO	NO	NO
ITG-SA	YES	NO	NO	NO
Standalone UCM	YES	NO	NO	NO
Standalone NRS	YES	NO	NO	NO

Table 9: Trap community string

Community string	Value
SYSMGMT_TRAP_COMM	Public
The trap community string applies to all system elements.	

Community strings are synchronized when you issue the **`sync snmpconf`** command.

SNMP CLI commands

The following table shows the CLI commands for configuring SNMP parameters.

Table 10: 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 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 Gateway Controller. The admingroup strings are 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.

=> Command	Description
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 • **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 NAV_SITE aa... a	Change the navigation site name, where • aa...a = a string with maximum length of 32 characters • default = Navigation Site Name

=> Command	Description
	Note: Use a single X to clear the field.
CHG NAV_SYSTEM aa... a	Change the navigation system name, where • aa...a = a string with a maximum length of 32 characters • default = Navigation System Name **Note:** Use a single X to clear the field.
CHG SELSIZE 5-(500)-2000	Changes the System Event List Size (the number of events in the SEL).
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).
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 on page 43.
NEW EPT aa... a CRITICAL x	Assigns a Critical severity to a new EPT entry, where

=> 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 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 • **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).

=> Command	Description
PRT ADMIN_COMM	Prints the administration group community strings. If you modify profiles without issuing the SYNC SNMPCONF command, the output displays the new configuration value as OVLY 117 Configuration and the current value as ACTIVE Configuration. After you issue the synchronization command, the OVLY 117 value is assigned to ACTIVE Configuration.
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 ENABLE_TRAPS	Prints the current value for the SET ENABLE_TRAPS configuration.
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 range of Event Preference Table (EPT) entries, where • **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 NAV_SITE	Print the navigation site name. If you modify profiles without issuing the SYNC SNMPCONF command, the output displays the new configuration value as OVLY 117 Configuration and the current value as ACTIVE Configuration. After you issue the synchronization command, the OVLY 117 value is assigned to ACTIVE Configuration.
PRT NAV_SYSTEM	Print the navigation system name If you modify profiles without issuing the SYNC SNMPCONF command, the output displays the new configuration value as OVLY 117 Configuration and the current value as ACTIVE

=> Command	Description
	Configuration. After you issue the synchronization command, the OVLY 117 value is assigned to ACTIVE Configuration.
PRT OPEN_ALARM	Prints the settings for all open SNMP traps (alarms). Only active slots are displayed. If you modify profiles without issuing the SYNC SNMPCONF command, the output displays the new configuration value as OVLY 117 Configuration and the current value as ACTIVE Configuration. After you issue the synchronization command, the OVLY 117 value is assigned to ACTIVE Configuration.
PRT SEL [nn[aaaa]]	Prints the most recent records in the system event list, where • **nn** = 0-(20)-SELSIZE. • [aaaa] = category name (for example, BUG) All categories are printed if not specified.
PRT SELSIZE	Prints the System Event List size.
PRT SNMP_SYSGRP	Print all parameters of the MIB-II system group. If you modify profiles without issuing the SYNC SNMPCONF command, the output displays the new configuration value as OVLY 117 Configuration and the current value as ACTIVE Configuration. After you issue the synchronization command, the OVLY 117 value is assigned to ACTIVE Configuration.
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. If you modify profiles without issuing the SYNC SNMPCONF command, the output displays the new configuration value as OVLY 117 Configuration and the current value as ACTIVE Configuration. After you issue the synchronization command, the OVLY 117 value is assigned to ACTIVE Configuration.
PRT TIMER	Prints the global timer window length (in minutes). See Global window timer length on page 43.
SET ENABLE_TRAPS aaa	Enables or disables the option to send SNMP traps, where

=> Command	Description
	aaa = ON or OFF
SET OPEN_ALARM <slot> <IP address> [port]	Add a SNMP (Simple Network Management Protocol) trap destination (Network Management System), where • <slot> = 0-7 • <IP Address> = any valid value in an x.x.x.x format (TCP/IP) • [port] = port number (if left blank, port 162 is used as the default) **Note:** To clear a SNMP trap destination, specify appropriate [slot] value and set [IP Address] = 0.0.0.0.
STAT SNMPCONF	This command returns the status of the SYNC SNMPCONF command. The returned results of this command are as follows: • SNMP Configuration is in progress—SNMP parameters have been modified through LD 117 and SYNC SNMPCONF command has not been executed. • SNMP Configuration is completed—SNMP parameters have been modified through LD 117 and SYNC SNMPCONF command has been executed.
SYNC SNMPCONF	Applies configured SNMP parameters to Call Server and propagates them to all elements with established links to the Call Server, such as SS, VGMC, and Gateway Controller. After this command is executed, PRT output listed as OVLY 117 Configuration is assigned to ACTIVE Configuration.
SYNC SYS	Synchronizes Dbconfig and QOS parameters. This command does not synchronize SNMP configuration parameters; use SYNC SNMPCONF.
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

=> Command	Description
	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: `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: Call Server (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 SNMP Profile Manager

This section describes how to configure SNMP on the primary UCM server using the SNMP Profile Manager interface.

Note:

Elements running Media Application Server (MAS) require additional separate configuration. For more information, see Media Application Server SNMP architecture on page 30.

You can manage SNMP by logging on to the primary UCM server and navigating to **Network > CS 1000 Servers > SNMP Profiles**. From this page you can access the SNMP Profile Manager or the SNMP Profile Distribution pages.

Adding a new MIBACCESS SNMP profile

Use this procedure to add a new MIBACCESS SNMP profile using the SNMP Profile Manager.

1. Navigate to **Network > CS 1000 Servers > SNMP Profiles**.

   The SNMP Profile Manager page displays.

2. Click **Add**.

   The New SNMP Profile page displays.

3. From the Profile Type menu, select **MIBACCESS**.

   The MIBACCESS profile configuration options appear, as shown in Figure 10: MIB Access SNMP profile configuration page on page 54.

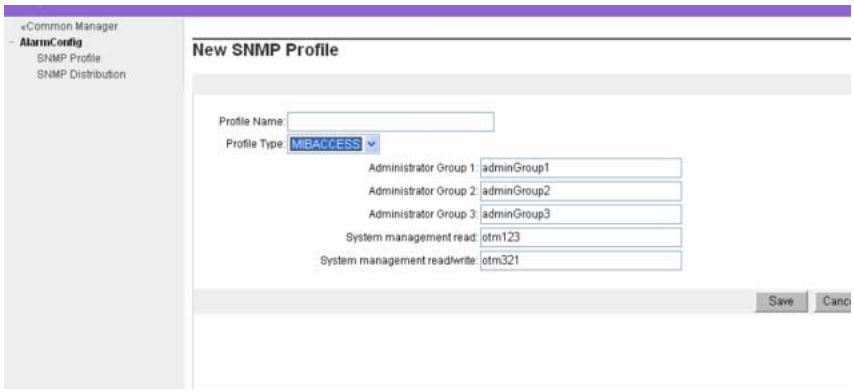


Figure 10: MIB Access SNMP profile configuration page

4. Configure the following options:
   - Administrator Group1
   - Administrator Group2
   - Administrator Group3
   - System Management Read
   - System Management Write
5. Click **Save**.

Adding a new SYSINFO SNMP profile

Use this procedure to add a new SYSINFO SNMP profile using the SNMP Profile Manager.

1. Navigate to **Network > CS 1000 Servers > SNMP Profiles**.

   The SNMP Profile Manager page displays.

2. Click **Add**.

   The New SNMP Profile page displays.

3. From the Profile Type menu, select SYSINFO.

   The SYSINFO profile configuration options appear, as shown in Figure 11: SYSINFO SNMP profile configuration page on page 55.

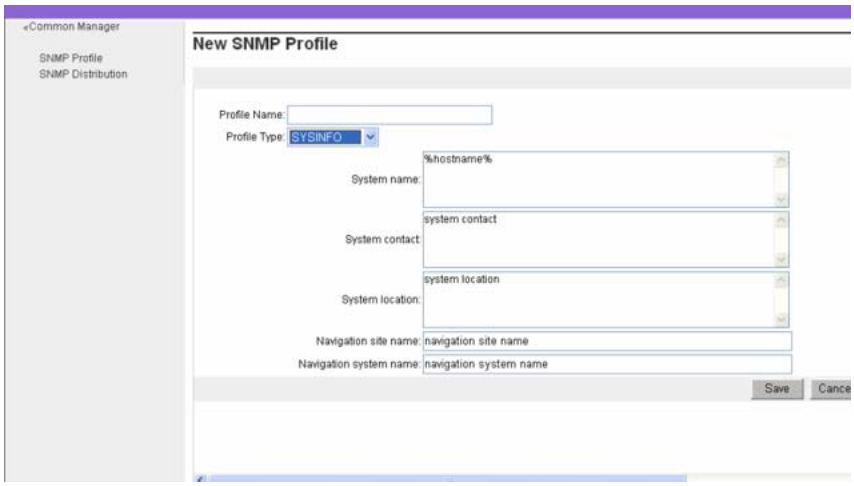


Figure 11: SYSINFO SNMP profile configuration page

4. Configure the following options:

   - System name
   - System contact
   - System location
   - Navigation site name
   - Navigation system name

5. Click **Save**.

Adding a new ALARM SNMP profile

Use this procedure to add a new ALARM SNMP profile using the SNMP Profile Manager.

1. Navigate to **Network > CS 1000 Servers > SNMP Profiles**.

   The SNMP Profile Manager page displays.

2. Click **Add**.
3. The New SNMP Profile page displays.
4. From the Profile Type menu, select **ALARM**.

   The ALARM profile configuration options appear, as shown in Figure 12: ALARM SNMP profile configuration page on page 56.

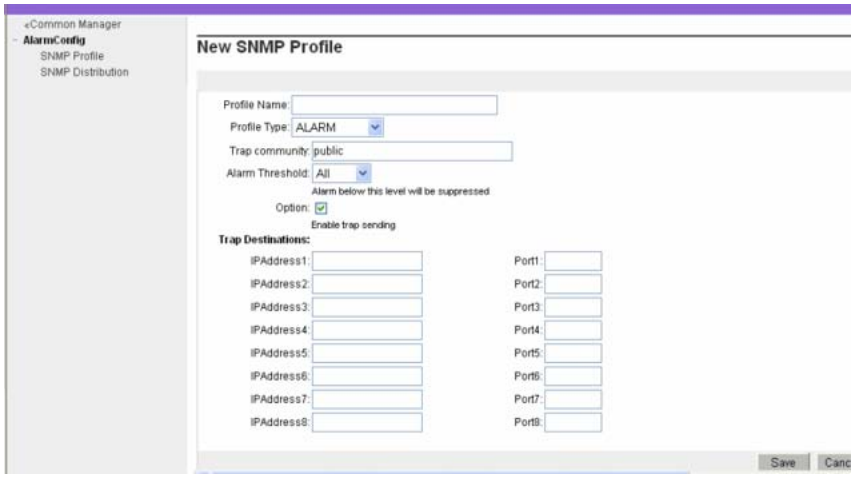


Figure 12: ALARM SNMP profile configuration page

5. Configure the following options:

   - Trap community
   - Alarm Threshold
   - Option to enable or disable trap
   - Trap Destinations with IP addresses and port numbers (maximum of eight)

6. Click **Save**.

Editing a MIBACCESS SNMP profile

Use this procedure to edit a MIBACCESS SNMP profile. Each SNMP profile is shown in the SNMP Profile Manager page as a link.

1. From the SNMP Profile Manager page, click the link of the MIBACCESS profile to modify.

   Note:
   You cannot modify a custom or default profile.

The SNMP MIB Access Profiles Details page appears.

The top section of the page provides the profile details for editing.

2. Make the required changes to the fields in the profile details section.
3. Click **Save**.

   The details are committed to the profile and propagated to the elements that currently use that profile.

   The bottom section of the page lists the elements that are currently associated with the profile. Each element also displays a status. When the elements are updated successfully with the changed profile data, the status appears as ASSIGNED. If an error occurs while updating profile to an element, the status appears as PENDING.

   If you modify the profile name, the version number is set to 1.0. If the profile name is not changed but you make modifications to any field in the profile, the version number increments by 1.0.

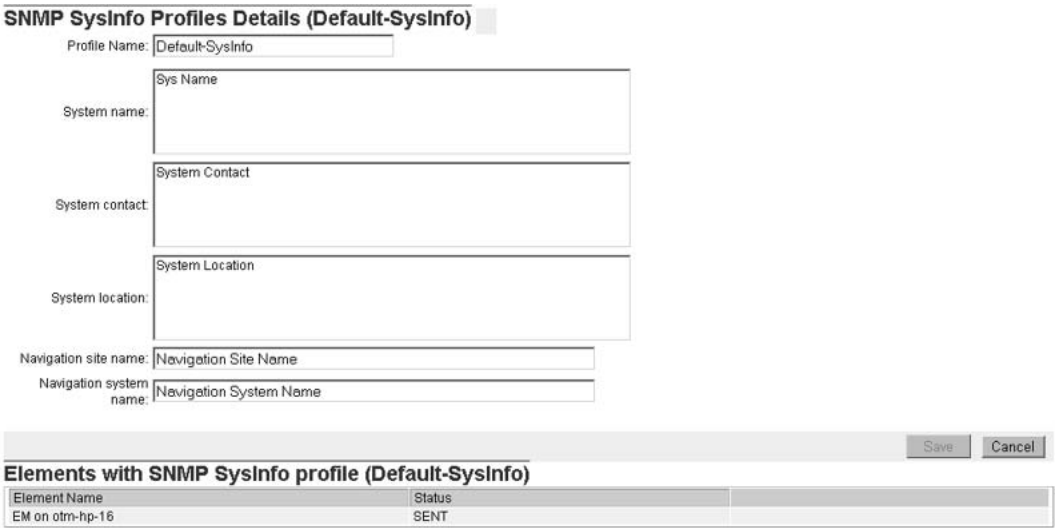
Editing a SYSINFO SNMP profile

Use this procedure to edit a SYSINFO SNMP profile. Each SNMP profile is shown in the SNMP Profile Manager page as a link.

1. From the SNMP Profile Manager page, click the link of the SYSINFO profile to modify.

   Note:
   You cannot modify a custom or default profile.

   The SNMP SysInfo Profiles Details page appears.



The top section of the page provides the profile details for editing.

2. Make the required changes to the fields in the profile details section.
3. Click **Save**.

   The details are committed to the profile and propagated to the elements that currently use that profile.

   The bottom section of the page lists the elements that are currently associated with the profile. Each element also displays a status. When the elements are updated successfully with the changed profile data, the status appears as ASSIGNED. If an error occurs while updating profile to an element, the status appears as PENDING.

   If you modify the profile name, the version number is set to 1.0. If the profile name is not changed but you make modifications to any field in the profile, the version number increments by 1.0.

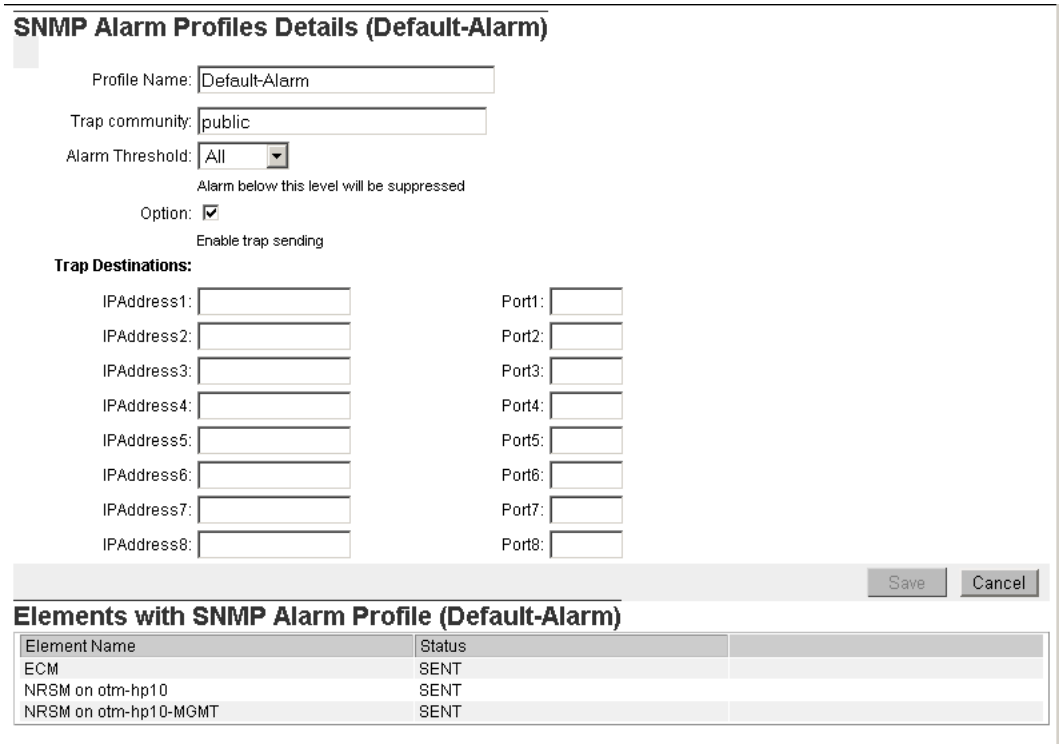
Editing an ALARM SNMP profile

Use this procedure to edit an ALARM SNMP profile. Each SNMP profile is shown in the SNMP Profile Manager page as a link.

1. From the SNMP Profile Manager page, click the link of the ALARM profile to modify.

   Note:
   You cannot modify a custom or default profile.

   The SNMP Alarm Profiles Details page appears.



The top section of the page provides the profile details for editing.

2. Make the required changes to the fields in the profile details section.
3. Click **Save**.

   The details are committed to the profile and propagated to the elements that currently use that profile.

   The bottom section of the page lists the elements that are currently associated with the profile. Each element also displays a status. When the elements are updated successfully with the changed profile data, the status appears as ASSIGNED. If an error occurs while updating profile to an element, the status appears as PENDING.

   If you modify the profile name, the version number is set to 1.0. If the profile name is not changed but you make modifications to any field in the profile, the version number increments by 1.0.

Deleting a SNMP profile

Use this procedure to delete a SNMP profile using the SNMP Profile Manager.

1. From the SNMP Profiles list, select the profiles to delete.
2. Click **Delete**.

If a profile selected for deletion is currently assigned to an element, a warning page appears stating that the profile is currently assigned and prompts for confirmation.

3. Click **OK** to delete the profile.

   Elements assigned to deleted profiles are assigned to the default profile. You cannot delete the default and custom profiles.

SNMP Profile Distribution

You can access the SNMP Profile Distribution page by clicking the **SNMP Distribution** link in the UCM navigator tree.

When you click the SNMP Profile Distribution link, the **Target Group Selection** page appears.

This page displays a list of system nodes in a navigation tree format. The nodes can be expanded to show the individual elements assigned to each node (only one node can be expanded at one time). Selecting a primary node causes the secondary nodes to be selected automatically. You can select up to a maximum of 500 elements. When you click **Next**, the SNMP Profile Distribution page appears

This page shows only Call Servers and the Primary and Member UCM servers. If a UCM server has an installed Signaling Server and an established PBXlink to a Call Server, it is not listed in the SNMP Profile Distribution Page because it receives SNMP parameters from the Call Server to which it is registered. This page displays the following information for the elements selected on the previous Target Group Selection page:

- Element Name
- IP address
- Current System Info profile
- Current MIB Access profile
- Current Alarm profile

From this page, you can assign profiles to elements. You can assign profiles to multiple elements. If you select a single element, the selections available in the Assign Profile Page list display only the currently associated profiles. If you select multiple elements, the list displays the profiles in alphabetical order with an option to configure a common profile for all of the selected elements.

The selected element names appear at the top of the lists separated by commas. If the element names exceed two lines, the list is prefixed with “…” to indicate the names are incomplete.

Note:

The SNMP Distribution page displays only Avaya Communication Server 1000 Release 6.0 and above elements. To configure SNMP parameters for devices installed for releases prior to Release 6.0, you must use the respective SNMP configuration methods for those releases.

Assigning SNMP profiles to elements

Use this procedure to assign SNMP profiles to elements.

1. From the UCM navigation menu, click **SNMP Profiles**.
2. Click **SNMP Profile Distribution**.

   The Target Group Selection page appears.
3. From the Target Group Selection page, select the elements to which you want to assign profiles. You can select elements within a group individually or select all elements within a group by selecting the top-level (parent) group.
4. Click **Next**.

   The SNMP Profile Distribution page appears.
5. From the SNMP Profile Distribution page, select the elements to which you want to assign profiles.
6. Click **Assign**.

   The SNMP Profile Distribution Details page appears, as shown in Figure 13: SNMP Profile Distribution Details page on page 61. From this page you can change any of the profiles shown in the SysInfo, MIB Access, or Alarm profile drop down lists. You can also click **View** to review the details of selected profiles.

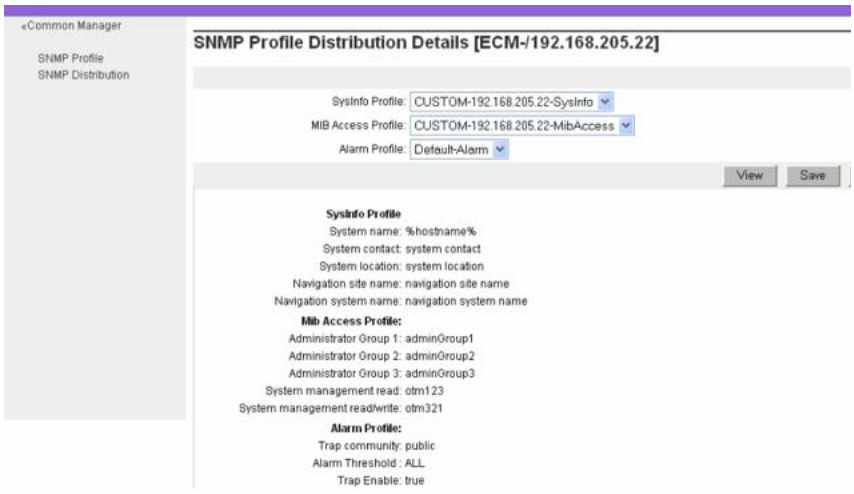


Figure 13: SNMP Profile Distribution Details page

7. Click **Save** to apply the profiles to the selected elements.

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 Gateway Controllers. Use Element Manager to configure SNMP trap destinations and community strings for Avaya Communication Server 1000 systems.

Note:

Elements running Media Application Server (MAS) require additional separate configuration. For more information, see Media Application Server SNMP architecture on page 30.

Any changes to SNMP parameters are detected by the SNMP Profile Manager in UCM, which creates a custom profile. A custom profile is created by the SNMP Profile Manager whenever SNMP parameters are configured using LD 117 or the SNMP configuration pages in Element Manager.

Note:

If a Call Server already has an assigned profile from the SNMP Profile Manager, that profile is replaced with the custom profile. No warning message is displayed when a preassigned profile is replaced with a custom profile.

For information about community strings, see Community strings on page 45.

Configuring SNMP on the Call Server

Use this procedure to configure SNMP on the Call Server.

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

   The SNMP Configuration page appears, as shown in Figure 14: Element Manager SNMP Configuration page on page 63.

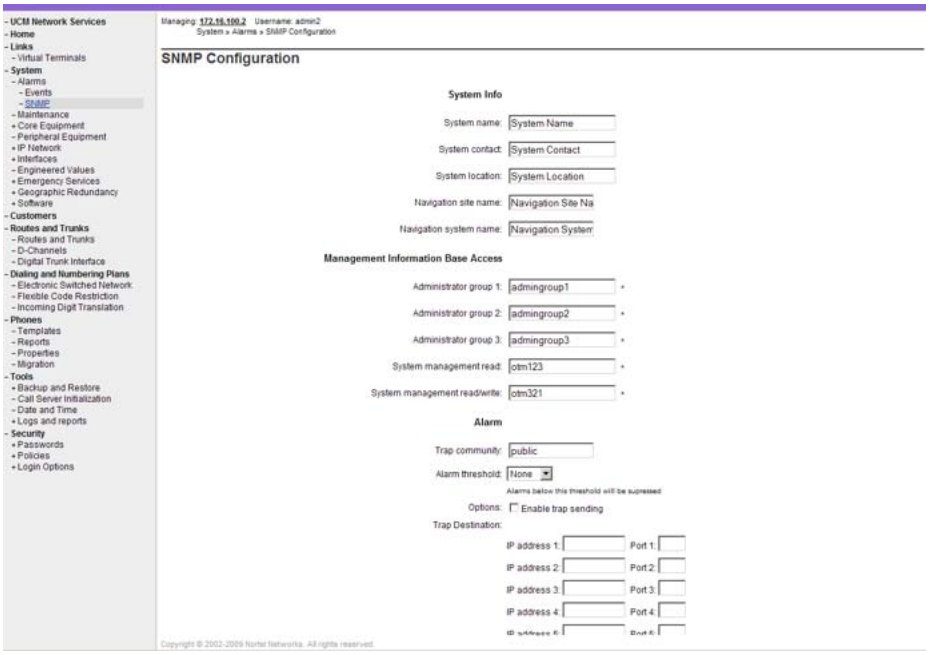


Figure 14: Element Manager SNMP Configuration page

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

   - System Name (%hostname%)
   - System Contact (SNMP_SYSCONTACT)
   - System Location (SNMP_SYSLOC)
   - Navigation Site Name (NAV_SITE)
   - Navigation System Name (NAV_SYSTEM)
   - Admin Groups 1-3 community strings (ADMIN_COMM).
   - System Management Read community string (SYSMGMT_RD_COMM)
   - System Management Write community string (SYSMGMT_WR_COMM)
   - System Management Trap community string (SYSMGMT_TRAP_COMM)
   - SNMP trap destination addresses and ports

   Note:
   All community strings, except the Trap community string, must be unique.

3. From the Alarm Threshold list, select the desired threshold. The options are Major, Minor, Critical, or None.
4. To enable trap sending, select the **Options** check box.
5. In the **Trap destination** fields, enter the IP addresses and ports of the trap destinations.

SNMP traps are sent to the IP addresses indicated here. If you do not specify a port for an IP address, port 162 is used as the default.

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

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

You can enter a maximum of eight trap destinations. They are numbered from 1 to 8.

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.

6. Click **Save** to save and synchronize the configuration.

   This action propagates the configuration settings to all network elements with an established PBXlink to the Call Server. It also propagates the configuration settings to UCM and replaces the profile associated with that Call Server with the custom profile in the SNMP Profile Manager. On the SNMP Distribution Page, a message appears indicating that the custom profile created through EM will replace the network level profile.

   You can also click **Cancel** to cancel the entry.

Chapter 6: Traps

Contents

This chapter contains information about the following topics:

Overview

In general, an Avaya Communication Server 1000 or Meridian 1 SNMP trap contains the following data:

- ELAN IP address of the element 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 trap OIDs provides a common format for all elements.

For more information, see MIBs on page 73.

Standard traps

In addition to the Avaya traps that are sent using the Common Trap format, other traps are sent by Avaya Communication Server 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 *Avaya Software Input/Output System Messages, NN43001-712*. The classification is based on the event category, such as ITG or ITS.

Avaya Software Input/Output System Messages, NN43001-712 also provides a list of critical traps that should be monitored by a 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 on page 45.

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.
- 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 Figure 15: SNMPv1 trap PDU fields on page 68.

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 *Avaya Software Input/Output System Messages, NN43001-712*.

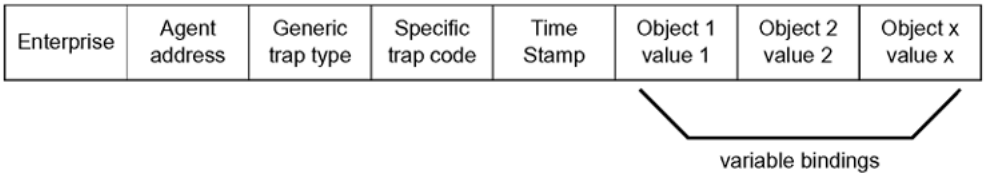


Figure 15: SNMPv1 trap PDU fields

Trap handling process

Table 11: Trap handling process on page 68 describes the trap handling process.

Table 11: 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 element.
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 Gateway Controller 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 format

ITG and ITS traps are in Common Trap MIB format, 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 = Info 6 = Indeterminate 7 = Cleared

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

For a detailed list of the ITG and ITS error messages, see *Avaya 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
- ITS
- QOS

View system error messages in CS 1000 systems

In Avaya Communication Server 1000 systems, a system error message is issued from the Signaling Server, Voice Gateway Media Card, or Gateway Controller 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 *Avaya Element Manager System Administration, NN43001-632*.

Test trap tool for Linux Base

System administrators can use a Linux base command to confirm if traps are being properly sent to the configured destinations. The **sendSnmpTrap** command generates a SNMP trap in Common-MIB format.

You must specify the full path when executing this command. The syntax for the command is as follows:

sendSnmpTrap <trap severity> <error code> <alarm type> <alarm data> <component> <notification ID> <probable cause>

Parameter	Description
<trap severity>	Numeric value indicating the severity of the trap. The following values are defined in common trap MIBs: • critical (1) • major (2) • minor (3) • warning (4) • info (5) • indeterminate (6) • cleared (7)
<error code>	Error code to be sent in trap, in the format AAA[A]NNNN, where: • A represents alphabetic characters • N represents numeric values
<alarm type>	Numeric value defining the type of alarm. Common trap MIB values are as follows: • communications (1) • qualityOfService (2) • processing (3) • equipment (4) • security (5) • operator (6) • debug (7) • unknown (8)
<alarm data>	String defining a description of the alarm.

Parameter	Description
	If using multiple words, enclose the entire string within double quotes. You do not need quotes for single words.
<component>	String denoting a component, in the format <Navigation System Name>:<Navigation Site Name>:<Component Name> If using multiple words, enclose the entire string within double quotes. You do not need quotes for single words.
<notification ID>	Integer denoting the unique ID for each generated trap, used for clearing alarms.
<probable cause>	Integer indicating the probable cause for the alarm. This value qualifies the alarm type field.

The return values for the **sendSnmpTrap** command are as follows:

- 0 —successful operation
- 1 —failure
- 2 —insufficient number of arguments
- 3-9 —invalid argument, with 3 being the first argument, 4 the second argument, and so on.

Corrective actions

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

- *Avaya Communication Server 1000M and Meridian 1 Large System Maintenance, NN43021-700*
- *Avaya Communication Server 1000E Maintenance, NN43041-700*
- *Avaya 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.
- Depending on how the trap was configured, use the CLI or Element Manager on the Call Server or SNMP Profile Manager to see if the trap has a lesser severity than the minimum severity threshold.
- 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.

Chapter 7: 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 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 a 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

Table 12: First four ASN.1 Object Types on page 74 lists the Object Types for the first four numbers of an OID that uses ASN.1 syntax.

Table 12: 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.

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 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 Avaya is 6889.

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 a 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)

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. Table 13: system objects on page 76 lists some of the common objects in the system group.

Table 13: 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 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>"` (c) Avaya Inc.

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

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
- VGMC

- Expansion Call Server - Normal mode, Sys XXXX
- Expansion Call Server - Survival mode, Sys XXXX
- Gateway Controller
- MG 1000E-SSC
- For Linux components, the SW field is populated as follows:

  SW: <application installed>,<UCM server mode>

Note:

If multiple applications are on the server, SW: pertains to the main use of the server. <application installed> can be one of the following (or blank if no application is installed):

- CS
- CS1000HS-EM
- SS_EM_SubM
- BRIDGE
- SubM
- EM
- SS
- SS_EM
- NRS
- NRS+SS
- NRS+SS_EM
- CS+SS+EM
- CS+SS+NRS+EM
- SIPL
- CS+SS+NRS+EM_SubM

<UCM server mode> can be one of the following (or blank if no server is configured):

- Primary Security Server
- Member server
- Backup server

Where BN: is one of the following:

- X.XXY for Call Server
- X.XX.XX for Signaling Server
- IPL-X.XX.XX for VGMC
- mgcYYYXX for Gateway Controller
- X.XX.XX for NRS/UCM 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 P4
- CP PM (Call Server)
- CP PM (Signaling Server)
- CP DC (Signaling Server)
- ITG-SA
- MGC
- MG XPEC
- CP MG
- MC32S
- HP DL320 for NRS/UCM on Linux
- IBM 306M for NRS/UCM on Linux
- HP-DL320-G4 for Signaling Server COTS
- IBM-x306m for Signaling Server COTS
- DELL R300
- MG 1010
- MG XPEC (NTDW20AAE6)
- SSMG (CP MG)

Examples:

PR: `"CS 1000E"` SW: `"Call Server, Sys 4021"` BN: `"6.0"` HW: `"CP-PM"` (c) Avaya Inc.

PR: `"CS 1000"` SW: `"SS_EM, Primary Security Server"` BN: `"6.00.11"` HW: `"IBM X3350"` (c) Avaya Inc.

(This example shows no application installed for SW field) PR: `"CS 1000"` SW: `"Member Server"` BN: `"6.00.16"` HW: `"Avaya CPPMv1"` (c) Avaya Inc.

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.

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

Supported MIBs

Table 14: Supported MIBs on page 80 lists the MIBs supported on the Avaya Communication Server 1000 and Meridian 1 systems. There is no difference between the enterprise-specific MIBs for Meridian 1 and Avaya Communication Server 1000 systems, except that there are no Signaling Server MIBs on Meridian 1 systems.

Table 14: 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 - hrDevice group - hrSWRun group - hrSWRunPerf group **Note:** Only certain objects in the Host Resources subgroups are supported.	• Avaya Proprietary MIBs • QOSTRAFFIC-MIB—provides similar information as QOS-MIB on 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)	QOS-MIB.mib **Note:** QOS-MIB.mib is also known as Zonetrafficrpt MIB - Signaling Server only.

	MIB-II groups	Other
	• 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.	
Linux		UCD-SNMP-MIB

Table 15: Definition of MIBs on page 81 defines the various MIBs.

Table 15: Definition of MIBs

MIB	Definition
Call Server MIB	
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 on page 76 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.

MIB	Definition
	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.
SNMP group	A collection of objects providing basic information and control of a 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

MIB	Definition
	- 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
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; it describes the number of connection sessions (for example, Telnet, Rlogin, SSH, FTP) 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

MIB	Definition
	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. 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. Avaya 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 • cd0: cd drive, no need to monitor

MIB	Definition
	• 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. - 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

MIB	Definition
	`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 This description applies to Call Servers on VxWorks platforms as CPU utilization is displayed on Call Servers using Linux. 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. 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 *Avaya Traffic Measurement Formats and Output Reference, NN43001-750*.
	hrSWRun Group:

MIB	Definition
	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: i. running(1) ii. runnable(2) but waiting for resource (such as CPU, memory, IO) iii. notRunnable(3) – loaded but waiting for event iv. invalid(4) – not loaded **Note:** Values are read-only. **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.
QOSTRAFFIC MIB group	QOSTRAFFIC-MIB provides information similar to the Zone Traffic reports generated by QOS-MIB on the Signaling Server. Both interzone and intrazone traffic reports are provided.
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 on page 76 for a description and examples of the sysDecscr OID.

MIB	Definition
	sysObjectID:.1.3.6.1.4.1.562.3.14 (.iso.org.dod.internet.private.enterprises.nt.meridian.linuxplatform) **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	The default implementation of the HR MIB is used.
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 *Avaya Traffic Measurement Formats and Output Reference, 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. **Note:** In previous releases, an LAPW user account (snmpqosq) was required for QOS-MIB access. This account is no longer required.
Voice Gateway Media Card MIB	
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 on page 76 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

MIB	Definition
	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).
Media Gateway Controller	
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 on page 76 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).
Linux NRS and UCM	
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.

MIB	Definition
	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 on page 76 for a description and examples of the sysDecscr OID. **sysObjectID:**For NRS: .1.3.6.1.4.1.562.3.12 (.iso.org.dod.internet.private.enterprises.nt.meridian.nrs)For EM or UCM:.1.3.6.1.4.1.562.3.13 (.iso.org.dod.internet.private.enterprises.nt.meridian.ecm)For all other installations:.1.3.6.1.4.1.562.3.14 (.iso.org.dod.internet.private.enterprises.nt.meridian.linuxplatform) **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.

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.

The inclusion of the telephones in the Entity MIB is configured in LD 117. See Table 16: LD 117 telephone inventory in Entity MIB command on page 91.

Table 16: 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

Important:

Avaya Communication Server 1000 Release 7.5 enterprise-specific MIBs are

- COMMON-TRAP-MIB.mib
- QOS-MIB.mib (also known as the Zonetrafficrpt.mib)
- QOSTRAFFIC-MIB.mib (Call Server implementation of QOS-MIB.mib)

Download the latest version of the MIBs for Avaya products from www.avaya.com.

Follow the steps in Downloading the MIBs from the Avaya Web site on page 91 to download the MIBs.

Downloading the MIBs from the Avaya Web site

1. Under the **Support** 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 Avaya Communication Server 1000 MIBs are found under **Communication Servers - Enterprise Communication Servers**.
4. In **2... Select a product**, choose a system type.

5. In **3... and get the content**, choose **Software**.
6. The MIBs are found in the downloadable software list.

Trap handling approaches

Avaya recommends that you use a Network Management System (NMS) to accept traps directly from the system components. Use a NMS (for example, HP OpenView) to accept traps directly from the Avaya Communication Server 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 Communication Server 1000 or Meridian 1 component must be loaded into the NMS. See the Attention dialog box in Accessing MIBs on page 91 for the required MIB modules.

See also Directly accepting traps with Network Management Systems and HP OpenView on page 92.

As an alternative to a NMS, you can use the Visualization Performance and Fault Manager (VPFM) product to accept traps and provide additional fault management capabilities.

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 Avaya Communication Server 1000 systems.

HP OpenView

The common trap MIB (*COMMON-TRAP-MIB.mib*) is used to enable HP OpenView to accept traps directly from the Avaya Communication Server 1000 devices. For more information, see Configuring SNMP alarms in HP OpenView NNM on page 97.

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.

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 Table 17: LD 117 EDT and EPT commands on page 93.

Table 17: 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).

=> Command	Description
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).
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. The severity can be INFO, MINOR, MAJOR, or CRITICAL.
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 severity can be INFO, MINOR, MAJOR, or CRITICAL.

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 or Element Manager.

Backup and restore

LD 43

The LD 43 commands listed in Table 18: LD 43 backup and restore commands on page 95 enable a backup and restore of the Call Server system group MIB variables, System Navigation variables, community strings, and other data.

On Linux systems, backup and restore is performed using the **sysbackup** and **sysrestore** commands.

Important:
In Communication Server 1000 Release 5.5 and earlier, BKO backups to external storage devices do not retain EPT flags. Therefore, if you perform a restore operation using backup

data from a Communication Server 1000 Release 5.5 or earlier system, the following parameters must be reconfigured:

- Alarm suppression threshold (CHG SUPPRESS_ALARM)
- Global suppression value (CHG SUPPRESS)
- Global timer window (CHG TIMER)
- EDT mode (CHG EDT)

If the data being restored is from an Avaya Communication Server 1000 Release 6.0 or higher system, the settings for these parameters are retained and no reconfiguration is required.

Table 18: 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.
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 Table 19: LD 143 Small System backup and restore commands using a PC Card on page 96 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.

Table 19: 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 Table 20: LD 43 Large System backup and restore commands using floppy disks on page 96 enable the backup and restore of the system group MIB variables, System Navigation variables, community string, and other data using floppy disks.

Table 20: 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.

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.

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 on page 98 to configure events in HP OpenView.

Configuring events

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

   See Figure 16: Root window to Event Configuration on page 99.

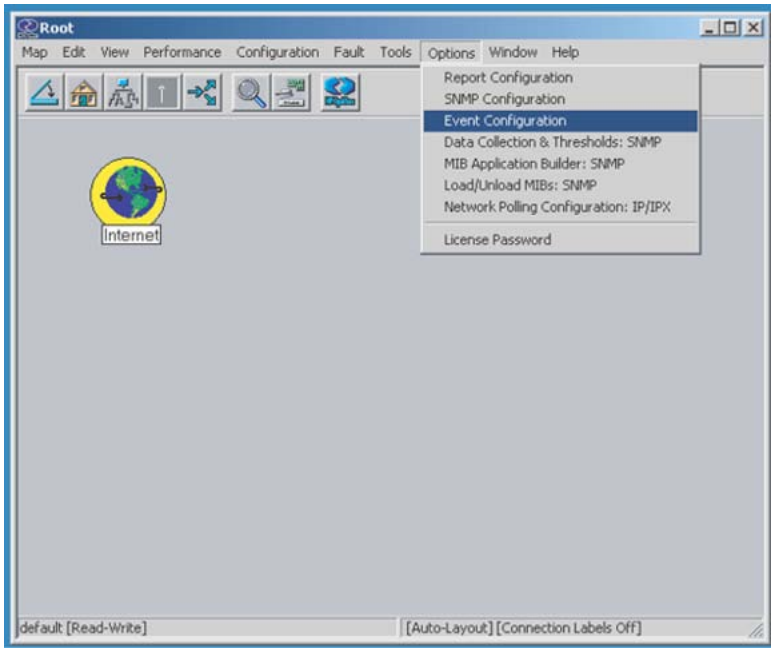


Figure 16: Root window to Event Configuration

The Event Configuration window appears. See Figure 17: Event Configuration and Enterprises window on page 100.

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

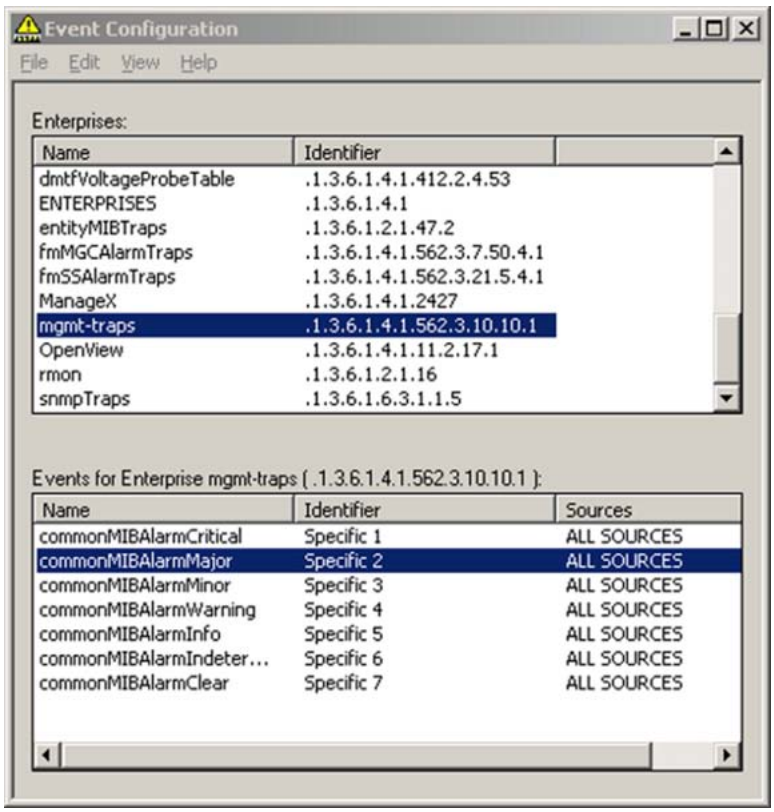


Figure 17: Event Configuration and Enterprises window

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 Figure 18: Modify Events window on page 101.

4. Configure the event as desired on the various tabs. For example, in the **Event Log Message** text box, shown in Figure 18: Modify Events window on page 101, 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.

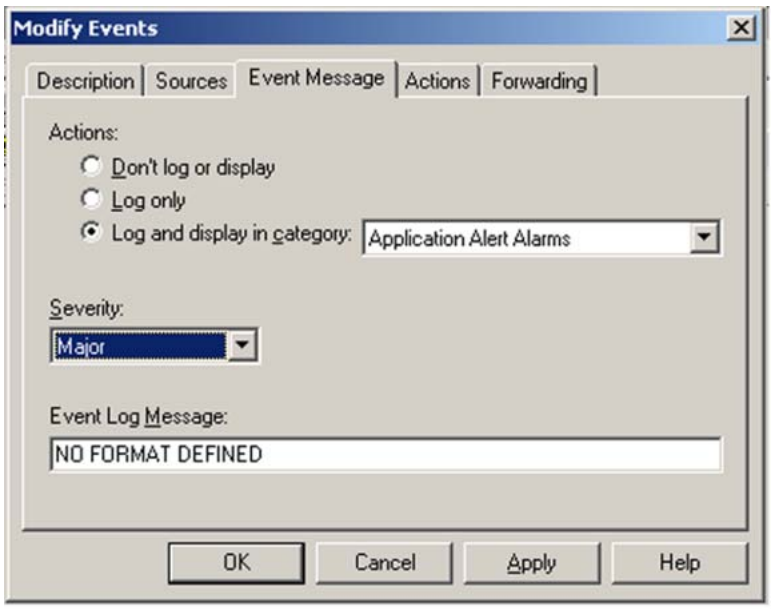


Figure 18: Modify Events window

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**.

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.

Other tools

You can now configure other tools, such as:

- paging alerts
- e-mail alerts
- event correlation

Appendix C: Common Trap Structure

Contents

This appendix contains information about the following topics:

Overview

A Common Trap structure ensures that traps from all Avaya Communication Server 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 Figure 15: SNMPv1 trap PDU fields on page 68. A trap type defines the severities, for example, *commonMIBAlarmMajor* or *commonMIBAlarmMinor*. See Common Trap MIB on page 109. The seven severities are

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

Table 21: Severity mapping table on page 104 compares the severity mapping of the Common Trap structure to the severity mapping used by the Call Server, Signaling Server, and Voice Gateway Media Card in Communication Server 1000 Release 5.0 and earlier.

In Avaya Communication Server 1000 Release 7.5, all CS 1000 devices use the Common Trap severity mapping.

Table 21: 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 Table 23: Variable binding mapping table on page 106.

- **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 Element Manager on the SNMP Configuration page.

The componentName is determined based on the original source of the trap. For mapping details for the system element and the component name, see Table 22: commonMIBComponentID mapping on page 105.

Table 22: commonMIBComponentID mapping

System elements	Component name
Call Server	CS
Signaling Server	SS
Voice Gateway Media Cards (includes MC32S)	VGMC
Media Gateway Controller	MGC
Media Gateway Extended Peripheral Equipment Controller	MGX
Common Processor Media Gateway	MGS
SIP NRS Linux	NRS
NRS Manager	NRSM
EM/BCC Linux	MGMT
Virtual Trunk on Linux	VTRK
Terminal Proxy Server on Linux	TPS
Shared Application on Linux	SSSHARED
Gatekeeper	GK
Sip Proxy Server on Linux	SPS
Network Connect Server on Linux	NCS
Connection Server	CSV
SIP Bridge	SIPBRG

- **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.

Table 23: Variable binding mapping table on page 106 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.

Table 23: 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	commonMIBAlarmType

Variable binding in Common Trap Structure	Variable binding in SS and VGMC	Variable binding in CS	Variable binding in Linux Trap
		ITU specification	
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

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 Avaya products from www.avaya.com/support.

Glossary

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.

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.

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

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

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 Avaya Communication Server 1000 Web server, Remote Procedure Call (RPC) Server, and Call Server.

Index

Special Characters

A

B

C

D

E

S

T

U

V

W

X

Z