SNMP Reference Guide for Avaya Communication Manager

03-602013
Issue 1.0
February 2007

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03-600758.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not 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. Customer and/or 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. 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 through the following Web site: http://www.avaya.com/support.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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

Contents

Chapter 1: SNMP Overview with Avaya Communication Manager

This document explains how SNMP works in an environment where Avaya devices are installed. It does not attempt to explain all of the many aspects of SNMP.

The SNMP protocol provides a simple set of operations that allow devices in a network to be managed remotely. The following versions of SNMP are supported by Communication Manager 4.0 and later releases:

- SNMP Version 1 (SNMP v1) and SNMP Version 2c (SNMP v2c): SNMP v1 was the initial version of SNMP. Security in SNMP v1 is based on plan-text strings known as communities. Communities are passwords that allow any SNMP-based application to gain access to a device's management information.
- SNMP Version 3 (SNMP v3): SNMP v3 provides additional security with authentication and private communication between managed entities.

SNMP is configured using the Communication Manager server's maintenance web interface. The server's web interface allows you to:

- View the G3-Avaya-MIB
- Configure the IP address for SNMP access to this server
- Enable and define SNMP Version 1 users and communities
- Enable and define SNMP Version 2c users and communities
- Enable and define SNMP Version 3 user names and passwords
- Add filters
- Add traps
- Test the delivery of a trap

For detailed information on how to administer SNMP on the Avaya server, see the *Administrator Guide for Avaya Communication Manager* (03-300508).

Managers and Agents

In SNMP there is a concept of a manager and an agent. This section explains how managers and agents work with Communication Manager.

Manager

A manager is a server running software that is used to manage a network. A manager can be referred to as a Network Management Station (NMS). An NMS either polls or receives traps from an agent. In an environment where an Avaya solution has been implemented, Avaya recommends using AIM. For more information on Avaya NMS offers, see *Avaya Integrated Management Overview* (14-300615).

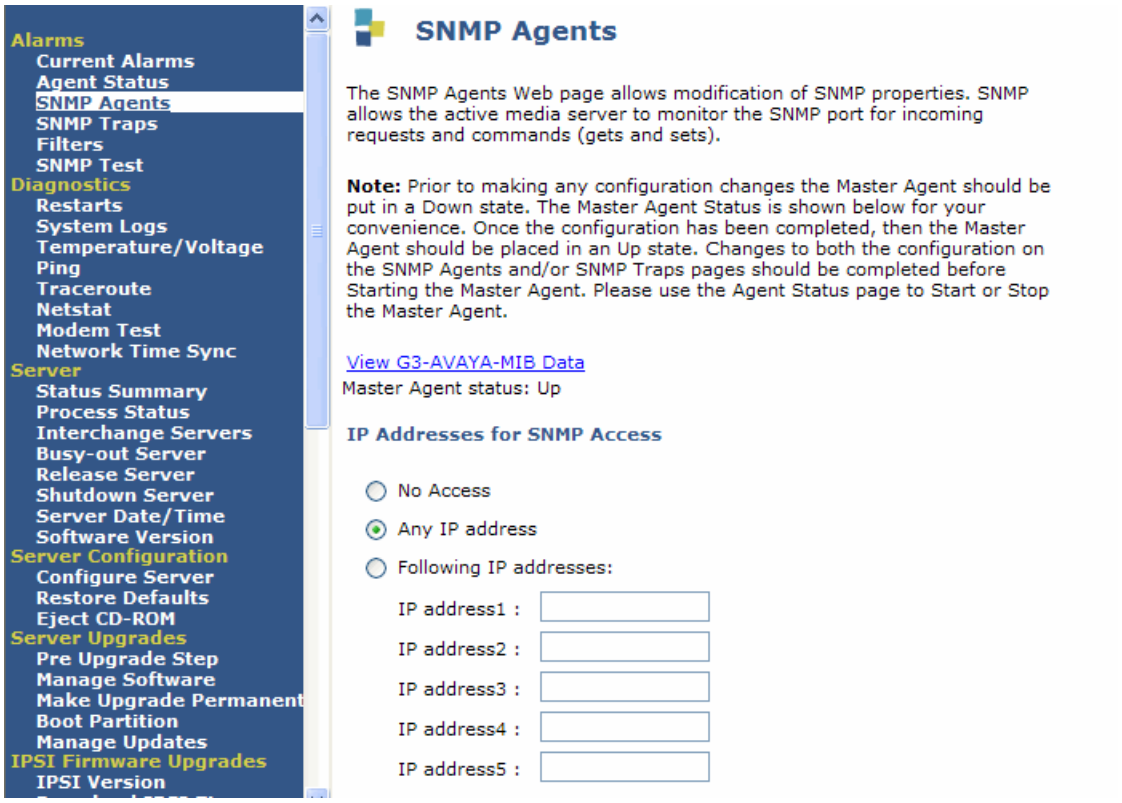
Agents

An SNMP agent is software that runs on the network device that you are monitoring. An SNMP agent performs the operational role of receiving and processing requests, sending responses to the manager, and sending traps when events occur.

Communication Manager uses the concept of a MasterAgent and subagents. A MasterAgent receives all the SNMP requests, responds to the SNMP requests, and sends the SNMP traps to the correct destination. If the MasterAgent is responding to an SNMP request, it validates the request to make sure that it has the right authentication to receive the data. If the request is valid, the MasterAgent either processes the request itself or forwards the request to the subagent responsible for providing the data. The subagents, once they have the data, communicate back to the MasterAgent with the requested data. The MasterAgent then sends the data back to the original requestor. In the case of SNMP traps, all the alarm traps come from one of the subagents called FPAgent (Fault and Performance agent). When a trap needs to be sent out, the FPAgent sends the trap to the MasterAgent and it forwards it to the administered trap destination.

During installation, Communication Manager installs two agents. One agent is used for reporting to Avaya services and cannot be configured. The other agent called the Communication Manager SNMP agent (CMSA) can be configured by clicking **SNMP Agents** under the **Alarms** heading in the server's web interface (see Figure 1). For information on how to administer an SNMP agent, see the *Administrator Guide for Avaya Communication Manager* (03-300508).

Figure 1: Configuring SNMP Agents on the Avaya server



Management Information Base (MIB)

A management information base (MIB) contains definitions and information about the properties of managed sources and services that an SNMP agent(s) supports.

The G3-Avaya-MIB is used for Communication Manager. The G3-Avaya-MIB contains:

- Object identifiers (IDs) for every Avaya object
- A list of MIB groups and traps along with their associated varbinds
- Configuration, fault and performance data associated with the Communication Manager server

To view the G3-Avaya-MIB, click **SNMP Agents** under the **Alarms** heading on the server's maintenance web interface. Click the link titled **View the G3-Avaya-MIB Data**.

Event ID

Server alarms contain event IDs. An event ID is used to identify a unique alarm or error condition for a particular alarm source, such as a hard disk or network interface card. The event ID is similar to the error numbers used by Communication Manager Maintenance Objects. For example, a DAJ1/DAL1 (duplication memory card) alarm in an S8700 Media Server has event IDs of 2, 3, 4, or 5. Each event ID has its own alarm level and description of the issue with the memory card.

Chapter 2: Traps

An SNMP trap is data that an agent sends to the NMS to let the NMS know that something has happened. A trap contains information only, such as alarm information generated by the server or an external device. A trap is the only type of message that an agent is capable of sending. All Communication Manager traps are defined in the G3-Avaya-MIB. This document addresses the traps that are generated from alarms only.

An alarm can be:

- Internal to Communication Manager, such as a trunk or station alarm
- External to Communication Manager, such as an uninterruptible power supply (UPS)
- A platform alarm, such as power or temperature

To view alarms:

- Use the SAT command **`display alarms`**
- Select **Alarms** > **Current Alarms** on the server's maintenance web page

A trap contains one or more varbinds. A varibind contains specific data that pertains to the trap. For example, in a trap for a major alarm there are varbinds that contain data about the name of the alarming server, the server's product ID, the alarm number, the alarm port, the alarm maintenance name (Maintenance Object or MO), the alarm type, etc. Table 1 contains a list of the most common Communication Manager traps. For a list of the varbinds associated with the traps in Table 1, see Table 3.

Configure trap destinations by clicking **SNMP Traps** under the **Alarms** heading on the server's maintenance web page. For information on how to configure a trap destination, see chapter 16 in the *Administrator Guide for Avaya Communication Manager* (03-300508).

Table 1 provides information on the trap types, the varbinds associated with each trap, and a description of what the trap is about. The information in Table 1 can be found in the G3-Avaya-MIB. For more information on the varbinds associated with the trap, see Table 3.

Table 1: SNMP Trap information

trap type	varbind	trap description
alarmClear	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber	A Cleared Alarm Notification has been issued by the switch indicating that all the alarms have been cleared.
alarmMajor	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	A major alarm was generated by the server.
alarmMinor	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	A minor alarm was generated by the server.
alarmWarning	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	A warning alarm was generated by the server.
		1 of 4

Table 1: SNMP Trap information (continued)

trap type	varbind	trap description
alarmResolved	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	An alarm was resolved on the server.
extalarmMajor	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3extdevAltName g3extdevDescription g3extdevID g3extdevBuilding g3extdevAddress g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	An external device major alarm was generated by the server. The varbinds describe the location and the nature of the alarm. An extalarmMajor trap applies to voice server alarms only.
extalarmMinor	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3extdevAltName g3extdevDescription g3extdevID g3extdevBuilding g3extdevAddress g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	An external device minor alarm was generated by the server. The varbinds describe the location and the nature of the alarm. An extalarmMinor trap applies to voice server alarms only.
		2 of 4

Table 1: SNMP Trap information (continued)

trap type	varbind	trap description
extalarmWarning	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3extdevAltName g3extdevDescription g3extdevID g3extdevBuilding g3extdevAddress g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	An external device warning alarm was generated by the server. The varbinds describe the location and the nature of the alarm. An extalarmWarning trap applies to voice server alarms only.
extalarmResolved	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsMaintName g3alarmsOnBrd g3alarmsAlarmType g3extdevAltName g3extdevDescription g3extdevID g3extdevBuilding g3extdevAddress g3alarmsIPAddress g3alarmsCategory g3alarmsErrorCodes	An external alarm has been resolved by the server. The varbinds describe the location and the nature of the alarm. An extalarmResolved alarm trap applies to voice server alarms only.
		3 of 4

Table 1: SNMP Trap information (continued)

trap type	varbind	trap description
alarmRMS	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3alarmsPort g3alarmsAlarmType g3alarmsCategory g3alarmsSrcIpAddr g3alarmsSrcMACAddr g3alarmsDestIPAddr g3alarmsDestPort g3alarmsProtocol g3alarmsCount g3alarmsViolationType g3alarmsCode g3alarmsData g3alarmsICMPType g3alarmsEventID g3alarmsStatus	An alarm that is associated with security related events has been generated by the server.
alarmRestart	g3clientExternalName g3alarmsProductID g3alarmsAlarmNumber g3restrartCraftDemand	A system restart has occurred on the server. The varbinds associated with the trap describe the location and the nature of the restrart.
		4 of 4

Chapter 3: Varbinds

A data field of a trap contains important information that identifies the reporting entity and the nature of the problem. This information is contained in one or more variable bindings (varbinds). A varbind associates a particular object instance with its current value. Table 2 shows the varbinds in an SNMP v1 trap Protocol Data Unit (PDU).

Table 2: The SNMPv1 Trap PDU

Trap data fields					**Varbinds**		
Enterprise	Agent address	Generic trap type	Specific trap code	Time stamp	Object 1 Value 1	Object 2 Value 2	Object x Value x

For example, when an ESS server took control of an IPSI that resides in port network four, a trap was sent that contained the following varbinds:

- g3clientsExternalName: NorthCampus
- g3alarmsProductID: 1000000000
- g3alarmsAlarmNumber: FPA:00000:1113081530:0000000000::N: (The following information breaks down each section of this string:)
  - FPA: The FPA before the first colon identifies that this trap was generated by the Fault and Performance Agent.
  - 1113081530: Indicates that the alarm was generated at 8:30 AM on November the 13th.
  - 0000000000: Indicates the date and time the alarm was resolved. In this example, the alarm is new so zeros are used in place of the data.
  - Null: The null string (::) is a place holder for the alternate name field. The alternate name fileld only applied to Communication Manager alarms and not platform alarms.
  - N: The ’N’ at the end of the string indicates that this is a new alarm. A modified alarm that is resent contains an ’M’.
- g3alarmsPort: ESS controlling IPSI PN4: cls 1
- g3alarmsMaintName: ESS
- g3alarmsOnBrd: 2
- g3alarmsAlarmType: min
- g3alarmsIPAddress: 198.122.255.301
- g3alarmsCategory: (NULL)
- g3alarmsErrorCodes: (NULL)

Table 3 provides a list of varbinds, a list of traps that contain this varbind, and a description of each varbind. The information in Table 3 can also be found in the G3-Avaya-MIB.

Table 3: Varbind information

Varbind name	Traps containing this varbind	Varbind description
g3clientExternalName	alarmClear alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved alarmRMS	g3clientExternalName contains the external name (host name) for the Communication Manager server.
g3alarmsAlarmNumber	alarmClear alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved alarmRMS	g3alarmsAlarmNumber contains a unique alarm number made up of the following information: • FPA: filter number. The filter number either contains the alarm filter number associated with the trap or ’00000’. • FPA: month alarmed • FPA: day alarmed • FPA: hour alarmed • FPA: minute alarmed • FPA: second alarmed • FPA: month resolved. If the alarm has not been resolved the month resolved contains 10 zeros. • FPA: day resolved. If the alarm has not been resolved the day resolved contains 10 zeros. • FPA: hour resolved. If the alarm has not been resolved the hour resolved contains 10 zeros. • FPA: minute resolved. If the alarm has not been resolved the minute resolved contains 10 zeros. • FPA: second resolved. If the alarm has not been resolved the second resolved contains 10 zeros. • FPA: alternate name field • FPA: new/modified flag
		1 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3alarmsProductID	alarmClear alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved alarmRMS	g3alarmsProductID contains a unique ten digit number that is associated with the server. The ten digit number is administered on the server using the /opt/ecs/bin/productid bash command. You can display the product ID in the server's maintenance web interface under the **Current Alarms** heading.
g3alarmsPort	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved alarmRMS	The information in g3alarmsPort differs depending on the kind of alarm: • Server alarm: If the alarm is a voice server alarm, g3alarmsPort contains the equipment location from which the alarm was generated. The syntax for the port number is, cabinet (01-44), carrier (A-E), slot (01-20), and port (02-32). • Platform or messaging alarm: If the alarm is a platform or messaging alarm, the g3alarmsPort displays the alarm description including the source of the alarm.
g3alarmsMaintName	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved	The information in g3alarmsMaintName differs depending on the kind of alarm: • Server alarm: If the alarm is a voice server alarm, g3alarmsMaintName contains the maintenance object (MO) name. Use the *Avaya Maintenance Alarm Reference* (30-300430) to find the maintenance procedure associated with this MO. • Platform or messaging alarm: If this is a platform or messaging alarm, g3alarmsMaintName contains a string indicating the resource from which the alarm was generated. Use the *Avaya Maintenance Alarm Reference* (30-300430) to find the maintenance procedure associated with this alarm source.
		2 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3alarmsOnBrd	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved	The information in g3alarmsOnBrd differs depending on the kind of alarm: • Server alarm: If the alarm is a voice server alarm, g3alarmsOnBrd contains a flag indicating whether or not the alarm generated from a circuit pack board. • Platform or messaging alarm: If this field is a platform or messaging alarm, g3alarmsOnBrd contains the event ID associated with the resource. Use the *Avaya Maintenance Alarm Reference* (30-300430) to find the maintenance procedure associated with the event ID or the circuit pack board.
g3alarmsAlarmType	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved alarmRMS	g3alarmsAlarmType contains the severity of the alarm such as major, minor, or warning. Use the *Avaya Maintenance Alarm Reference* (30-300430) to find the maintenance procedure associated with this alarm type.
g3extdevAltName	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved	g3extdevAltName contains the alternate name of the external device. For more information on external device alarms, see *Maintenance alarms for Avaya Communication Manager, Media Gateways and Servers* (03-300430).
g3extdevDescription	extalarmMajor extalarmMinor extalarmWarning extalarmResolved	g3extdevDescription contains the description of the external device. For more information on external device alarms, see *Maintenance alarms for Avaya Communication Manager, Media Gateways and Servers* (03-300430).
		3 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3extdevID	extalarmMajor extalarmMinor extalarmWarning extalarmResolved	g3extdevID contains the product identifier of the external device. For more information on external device alarms, see *Maintenance alarms for Avaya Communication Manager, Media Gateways and Servers* (03-300430).
g3extdevBuilding	extalarmMajor extalarmMinor extalarmWarning extalarmResolved	g3extdevBuilding contains the building location of the external device. For more information on external device alarms, see *Maintenance alarms for Avaya Communication Manager, Media Gateways and Servers* (03-300430).
g3extdevAddress	extalarmMajor extalarmMinor extalarmWarning extalarmResolved	g3extdevAddress contains the address of the external device. For more information on external device alarms, see *Maintenance alarms for Avaya Communication Manager, Media Gateways and Servers* (03-300430).
g3restartDateTime	alarmRestart	g3restartDateTime contains the date and time that the restart happened. The format for the date and time is MM/DD HH:MM.
g3restartLevel	alarmRestart	g3restartLevel contains the level of the restart. The level can be either warm, cold-2, reboot, or reload. Information on server restart levels can be found in the *Maintenance Commands for Avaya Communication Manager Media Gateways and Servers* (03-300431).
g3restartCarrier	alarmRestart	g3restartCarrier contains the carrier where the restart occurred. The carrier can either be carrier A or carrier B.
g3restrartCraftDemand	alarmRestart	g3restartCraftDemand contains a flag of yes (Y) or no (N) indicating if craft demanded the restart.
		4 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3restartEscalated	alarmRestart	g3restartEscalated contains a yes (Y) or no (N) flag that indicates if the server interchange was escalated. An escalation indicates that the current restart has been escalated or increased to a higher level. Information on server restart causes and escalations can be found in the *Maintenance Commands for Avaya Communication Manager Media Gateways and Servers* (03-300431).
g3restartInterchange	alarmRestart	g3restartInterchange contains a yes (Y) or no (N) flag that indicates if the server interchanged.
g3restartUnavailable	alarmRestart	g3restartUnavailable contains the amount of time in the form of HH:MM:SS that the server was unavailable due to the restrart.
g3restartCause	alarmRestart	g3restartCause contains the cause for the restart. For more Information on server restart causes, see *Maintenance Commands for Avaya Communication Manager Media Gateways and Servers* (03-300431).
g3vintageSpeArelease	alarmRestart	g3vintageSpeArelease contains the release number for SPE A. A release number is the Communication Manager release the server is running.
g3vintageSpeBrelease	alarmRestart	g3vintageSpeBrelease contains the release number for SPE B. A release number is the Communication Manager release the server is running.
g3vintageSpeAupID	alarmRestart	g3vintageSpeAupID contains the update identifier for SPE A. An update identifier is the update number(s) or patch number(s) currently installed on SPE A.
g3vintageSpeBupID	alarmRestart	g3vintageSpeBupID contains the update identifier for SPE B. An update identifier is the update number(s) or patch number(s) currently installed on SPE B.
		5 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3alarmsIPAddress	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved	g3alarmsIPAddress displays the IP address of the alarming server.
g3alarmsCategory	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved alarmRMS	A filter enables you to specify a set of parameters to filter out selected alarms that are sent as traps. To add a filter, select **Filters** under the **Alarms** heading on the server's maintenance web interface. When you add a filter, one of the parameters is called 'Category'. A category is a logical grouping of maintenance objects. For example, if you specify a category of stations, alarms for any maintenance object in that grouping causes a trap to be sent. For more information on how to add a filter, see, *Administrator Guide for Avaya Communication Manager* (03-300508). If the trap was created based on a filter that specified the Category parameter, g3alarmsCategory will be populated, otherwise g3alarmsCategory will be blank.
g3alarmsErrorCodes	alarmMajor alarmMinor alarmWarning alarmResolved extalarmMajor extalarmMinor extalarmWarning extalarmResolved	The error code string is a list of colon-separated codes that display the possible errors that may have caused the alarm. Some alarm types do not have error codes associated with them, such as a platform alarm. In this case, the g3alarmsErrorCodes field contains a null string.
g3alarmsSrcIpAddr	alarmRMS	g3alarmsSrcIpAddr contains the Internet Protocol (IP) address of the attack location.
		6 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3alarmsSrcMACAddr	alarmRMS	g3alarmsSrcMACAddr contains the Machine Access Code (MAC) address of the attack location.
g3alarmsDestIPAddr	alarmRMS	g3alarmsDestIPAddr contains the IP address of the attacked destination.
g3alarmsDestPort	alarmRMS	g3alarmsDestPort contains the IP address port of the attacked destination.
g3alarmsProtocol	alarmRMS	g3alarmsProtocol contains the Internet Control Message Protocol (ICMP), Transmission Control Protocol/Internet Protocol (TCP), or User Datagram Protocol (UPD) defined by the IP protocol the message.
g3alarmsCount	alarmRMS	g3alarmsCount contains the number of attacks or violations during the reporting time period.
		7 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3alarmsViolationType	alarmRMS	g3alarmsViolationType contains either the Denial of Service (DoS) attack type or login type. The following list contains the DoS types: • Not IP/ARP/802.1Q • Group MAC source address • Foreign host Address Resolution Protocol (ARP) • Group MAC ARP reply • Unknown ARP opcodes • Malformed ARP reply • IP with group MAC destination • Same IP source and destination • Rate limit ICMP • Fragmented ICMP • Unknown TCP port • TCP urgent packet • ICMP source quench • Bad IP vers/hdr length • Rate limit RAS port • Unknown DoS type The following list contains the login types: • SNMP • File Transfer Protocol (FTP) • TELNET • Secure Shell (SSH) • SNMP with source IP address • FTP with source IP address • TELNET with source IP address • SSH with source IP address
g3alarmsCode	alarmRMS	g3alarmsCode contains the ICMP code or ARP opcode.
g3alarmsData	alarmRMS	g3alarmsData contains the unformatted message data for unknown data format (not IP or ARP).
g3alarmsICMPType	alarmRMS	g3alarmsICMPType defines ICMP type in ICMP protocol format.
		8 of 9

Table 3: Varbind information (continued)

Varbind name	Traps containing this varbind	Varbind description
g3alarmsEventID	alarmRMS	g3alarmsEventID identifies the Managed Security Services (MSS) Event type. The following list contains the MSS Event types: • Security Violation Notification (SVN) station security code • SVN authorization code • SVN barrier code • Automatic Circuit Assurance (ACA) • Local Survivable Processor (LSP) registration notification • LSP unregistration • IP station unregistration • IP station registration invalid extension • IP station registration invalid password • Board DoS violation notification • Board login violation notification • IP board registration and unregistration
g3alarmsStatus	alarmRMS	g3alarmsStatus contains the status of the alarm - sent and/or acknowledged.
		9 of 9

Index

Index