Gateway Traps for the G250/G350/G430/G450/G700 Avaya S8xxx Servers

03-602803
Issue 2
May 2009

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 Websites 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 Website: 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 the 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").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS):
  End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU):
  End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU):
  End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User" means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (for example, webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR):
  Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (See Third-party Components for more information).

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 Website: http://support.avaya.com/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 Website:

http://www.support.avaya.com/.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to:securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

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.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

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

Contents

Contents

Avaya Media Gateway Traps

This document describes the Gateway Traps for the G250, G350, G450, and G700 Avaya Media Gateways.

A trap indicates a special condition that exists or an event that occurs within the system. Some traps indicate configuration changes or component modifications and are merely informative. Other traps indicate warning or error conditions that may compromise the performance of the media gateway. Serious traps trigger alarms which are communicated to an alarm management site.

Alarm Format

Media Gateways report alarms to the primary server (either an S8300, S8500, or S8700-series Server) using SNMP traps. Like the primary server's own alarms, alarms from a Media Gateway:

- Reside in the primary server's alarm log
- Can be viewed using the SAT command **`display alarms`**
- Can be viewed using the Web Interface Display Alarms option

However, the format of these displayed alarms is slightly different. As an example, a displayed alarm has the following format:

n CMG 1 WRN 07/17/2006:13:45 121.1.1.2:cmgMultipleFanFault

Within the above alarm-display string, the value:

- "n" is a sequential alarm ID.
- "CMG" identifies a Media Gateway as the maintenance object.
- "1" is the event's ID (1st column of Table 5: Media Gateway Traps and Resolutions).

This table also contains each alarm's corresponding SNMP trap # in the 2nd column. However, many of the MIB-defined traps have been excluded, either because:

- A specific trap (such as Trap #3) is the SNMP mechanism to clear an alarm logged by another specific trap (in this case, Trap #2).
- The specific event indicated by a trap is not severe enough to justify an entry in the primary server's alarm log.
- A trap is defined, but not implemented.
- A trap # is reserved for future use.

- “WRN” is the event’s severity (3rd column of Table 5: Media Gateway Traps and Resolutions).
- “07/17/2006:13:45“is the event’s date and time stamp.
- “121.1.1.2“is the IP address for Telnet access to the alarmed Media Gateway Processor (MGP).
- “cmgMultipleFanFault” is the trap name (4th column of Table 5: Media Gateway Traps and Resolutions).

SNMP Alarming on the Media Gateway

Setting up SNMP alarm reporting involves two main tasks:

- Configure the primary server to report alarms
- Configure the Media Gateway to send SNMP traps

Configure the primary server to report alarms

The primary server may be either an S8300, S8500, S8710, S8720, or S8730 server. The server supports two methods for reporting alarms. Either method, both, or no alarm-reporting method may be used at a given site.

- **OSS Method** - The server's software applications and hardware devices under its control can generate Operations Support System (OSS) alarms. These alarms are recorded in the server logs, and may be reported to Avaya's Initialization and Administration System (INADS) or another services support agency over the server's modem interface.

  To activate OSS alarm notification: The server requires a USB connection to a modem that is connected to an analog line. The modem must be configured using the Web Interface on the Set Modem Interface screen and enabled to send and receive calls using the Enable/ Disable Modem screen. Configuration of the OSS alarming method can only be done using Linux shell commands.
- **SNMP Method** - SNMP traps may be sent in User Datagram Protocol (UDP) to a corporate network management system (NMS) using the Configure Trap Destinations screen. The OSS and SNMP alarm-notification methods operate independently of each other. Either or both may be used. Currently, the following NMSs are supported:
  - Communication Manager Fault and Performance Manager, as a standalone application, or integrated within
  - Avaya Network Management Console with VoIP SystemView

- HP Openview

To activate SNMP alarm notification: On the server Web Interface, use the Configure Trap Destinations screen to set up SNMP destinations in the corporate NMS.

Add INADS Phone Numbers and Enable Alarms to INADS

The following procedure using the primary server's Linux shell commands administers the dial-out modem to send alarms in the OSS method. In this example, the primary server is an S8300, and the services support agency is Avaya's Initialization and Administration System (INADS).

Note:

Perform this task after all Communication Manager administration is complete.

To add INADS phone numbers and enable alarms to INADS

1. Connect the laptop to the Services port of the S8300 Server

   Note:

   Perform these steps only if the S8300 is the primary controller and the customer has a maintenance contract with Avaya. Use the information acquired from the ART tool. See "*Run the ART Tool for the INADS IP Address*" in *Installing and Upgrading the Avaya S8300 Server (555-234-100)* and *Installing and Upgrading the Avaya G700 Media Gateway (03-603333)*. Also, a USB modem must have already been installed. See "*Universal Serial Bus (USB) Modems*" in the same source.

2. Click **Start > Run** to open the Run dialog box
3. Enter **`telnet 192.11.13.6`**
4. Log in as **craft**.
5. At the prompt, enter **`almcall -f`** ***`INADS phone number`*** **`-s`** ***`second-number`***
6. At the prompt, enter **`almenable -d b -s y`**
7. Enter **`almenable`** to verify that the alarms are enabled.
8. Log off.

Configure the Media Gateway to send SNMP traps

See G250/G350 Traps for configuring, sending, and resolving traps specific to the G250/G350 Media Gateway.

See G450/G700 Traps for configuring, sending, and resolving traps specific to the G450/G700 Media Gateway.

G250/G350 Traps

This section describes the set of traps that are defined for the Avaya G250/G350 Media Gateway.

SNMP management is a function of the Avaya MultiService Network Manager. For additional information, including information on event logs and trap logs, please refer to the *Avaya P333T User's Guide*.

The Dynamic Trap Manager feature of the G250/G350 insures that SNMP traps and alarms are always sent to the currently active Media Gateway Controller. By default, the Dynamic Trap Manager sends all SNMP messages to the currently active MGC. The Dynamic Trap Manager can be configured to manage only a subset of SNMP messages using the **`snmp-server dynamic-trap-manager`** CLI command.

Configuring the G250/G350 to send SNMPv3 alarms

The Avaya G250/G350 Media Gateway uses SNMPv3 for traps and alarms. In order to configure the Avaya G250/G350 Media Gateway to send SNMP traps to the primary server you must enable the SNMP agent, specify the SNMP host, and setup SNMP authentication. You perform these tasks using the following CLI commands:

- To enable the SNMP agent: **`ip snmp-server`**
- To specify the SNMP host: **`snmp-server host`**
- To create an SNMPv3 view: **`snmp-server view`** ***`viewname subtree`***
- To create an SNMPv3 group and specify its views: **`snmp-server group`** ***`groupname`*** **`read`** ***`readviewname`*** **`write`** ***`writeviewname`*** **`notify`** ***`notifyviewname`***
- To create a user and add the user to a group: **`snmp-server user`** ***`username groupname`***

Configure the host for G250/G350 SNMP traps

Events occurring on the G250/G350 cause SNMP traps to be generated. The Avaya G250/G350 Media Gateway can be configured to send SNMP traps to any network management system (NMS) in the network, including the primary server. You specify the destination host using the G250/G350 CLI **`snmp-server host`** command. The traps are sent in User Datagram Protocol (UDP) on the customer's IP network.

The command syntax is:

```
snmp-server host {<hostaddress>|<hostname>} {traps|informs}
{{{v1|v2c} <community> | {v3 [auth|noauth|priv] <user>}} [udp-port
<port>] [<notification-type-list>]
```

This command is used both to specify the destination host for SNMP messages, and to define which SNMP messages are to be sent.

For example, to enable the SNMPv3 manager at IP address 192.16.55.126 to receive inform-type messages, to use SNMPv3 authentication, and to receive Ethernet port fault notifications only, enter:

```
G350-001(super)# snmp-server host 192.16.55.126 informs v3 auth localuser
eth-port-faults
```

Note:

You must log in to the CLI as **admin** to administer SNMP settings.

Refer to Table 1: SNMPv3 Notification Types for a full list of notification types that can be configured.

Table 1: SNMPv3 Notification Types ***1 of 2***

Notification Type	Description
all	All notifications
generic	Generic traps
hardware	Hardware faults
rmon	RMON rising/falling alarm
dhcp server	DHCP server error, such as a DHCP IP conflict detection or notification of no IP address left for specific network
dhcp-clients	DHCP client error, such as a DHCP client conflict detection
rtp-stat-faults	RTP statistics: OwS fault/clear traps
rtp-stat-qos	RTP statistics: end-of-call QoS traps
wan	WAN router traps
media-gateway	Media gateway traps (equivalent to MGP traps)
security	Security traps, such as unAuthAccess, macSecurity, unknownHostCopy, and accountLockout
config	Configuration change notifications
eth-port-faults	Ethernet port fault notifications
sw-redundancy	Software redundancy notifications

1 of 2

Table 1: SNMPv3 Notification Types *2 of 2*

Notification Type	Description
temperature	Temperature warning notifications
cam-change	Changes in CAM notifications
policy	Changes in policy (L3 devices) notifications
link-faults	ITC proprietary link down notifications
supply	Power supply (main and backup) notifications
	2 of 2

Configure SNMPv3 authentication

In order to use SNMPv3 authentication, you must create users, groups, and views for the G250/G350.

The G250/G350 provides several pre-configured views and groups for setting up SNMP authentication. Refer to Table 2: G250/G350 pre-configured views and Table 3: G250/G350 pre-configured groups for a description of these objects and how they can be used.

Table 2: G250/G350 pre-configured views

Viewname	Description
snmpv1View	A view for backwards compatibility with v1 SNMP users, providing v1 level access only.
v3ConfigView	A view for an SNMPv3 user with non-administrative privilege. USM and VACM table access is restricted to changing password and all download copy config commands.
restricted	A view providing limited access to SNMP objects. Access is restricted to the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtreees.
iso	A view providing maximal access, for users with admin privileges.

Table 3: G250/G350 pre-configured groups *1 of 2*

Group Name	Security Model	Security Level	Read View Name	Write View Name	Trap View Name
ReadCommG	v1	1 (noAuthNoPriv)	snmpv1View		snmpv1View
ReadCommG	v2	1 (noAuthNoPriv)	snmpv1View		snmpv1View
WriteCommG	v1	1 (noAuthNoPriv)	snmpv1View	snmpv1View	snmpv1View
					1 of 2

Table 3: G250/G350 pre-configured groups ***2 of 2***

Group Name	Security Model	Security Level	Read View Name	Write View Name	Trap View Name
WriteCommG	v2	1 (noAuthNoPriv)	snmpv1View	snmpv1View	snmpv1View
v3ReadWriteG	v3 (USM)	3 (AuthPriv)	v3configview	v3configview	v3configview
v3ReadOnlyG	v3 (USM)	3 (AuthPriv)	v3configview		v3configview
initial	v3 (USM)	1 (noAuthNoPriv)	restricted	restricted	restricted
v3AdminViewG	v3 (USM)	3 (AuthPriv)	iso	iso	iso

2 of 2

G250/G350 traps and resolutions

Although these alarms can be viewed from the primary server, they are normally resolved from within the Avaya G250/G350 Media Gateway. The G250/G350 generates the following traps. Follow the error resolution procedures in Table 4: G250/G350 Traps and Resolutions to resolve errors indicated by these traps.

Table 4: G250/G350 Traps and Resolutions ***1 of 16***

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
snmpTraps	1	coldStart	Boot	Warning	The entity is reinitializing itself in such a way as to potentially cause the alteration of either the agent's configuration or the entity's implementation. This trap is always enabled.
snmpTraps	2	warmStart	Boot	Warning	The entity is reinitializing itself in such a way as to keep both the agent's configuration and the entity's implementation intact. This trap is always enabled.
snmpTrap	3	linkDown	System	Warning	There is a failure in one of the communication links in the agent's configuration.
snmpTraps	4	linkUp	System	Warning	One of the communication links in the agent's configuration has come up.
snmpTrap	5	authenticFailure	Security	Notification	The protocol is not properly authenticated.
rmon	1	risingAlarm	Threshold	Warning	An alarm entry has crossed its rising threshold.
rmon	2	fallingAlarm	Threshold	Warning	An alarm entry has crossed its falling threshold.
frame-relay	1	frDLCIStatusChange			A DLCI has been created or deleted, or has state changes.

1 of 16

Table 4: G250/G350 Traps and Resolutions *2 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avayaG350	1	config			The configuration has been changed.
avayaG350	2	fault			A fault has been generated.
avayaG350	12	deleteSWRedundancyTrap	Switch Fabric	Info	A redundancy link has been deleted.
avayaG350	13	createSWRedundancyTrap	Switch Fabric	Info	A redundancy link has been created for the specified ports.
avayaG350	27	duplicateIPTrap	Router	Warning	A duplicate IP address has been identified.
avayaG350	30	wanPhysicalAlarmOn	Wan	Critical	An E1/T1 serial cable has been disconnected.
avayaG350	31	wanPhysicalAlarmOff	Wan	Notification	An E1/T1 serial cable has been reconnected.
avayaG350	32	wanLocalAlarmOn	Wan	Error	A local alarm (such as LOS) has been generated.
avayaG350	33	wanLocalAlarmOff	Wan	Notification	A local alarm (such as LOS) has been cleared.
avayaG350	34	wanRemoteAlarmOn	Wan	Error	A remote alarm (such as AIS) has been generated.
avayaG350	35	wanRemotetAlarmOff	Wan	Notification	A remote alarm (such as AIS) has been cleared.
avayaG350	36	wanMinorAlarmOn	Wan	Warning	
avayaG350	37	wanMinorAlarmOff	Wan	Notification	
avayaG350	60	IntPolicyChangeEvent	Policy	Info	The active policy list for the specified device or module has changed.
avayaG350	62	ipPolicyAccessControlListLvlRuleTrap	Policy		A packet fragment has been denied access on the specified interface
avayaG350	64	IntPolicyAccessControlViolationFit	Policy	Warning	A packet has violated a policy rule on the specified interface. The trap includes information about the slot where the event occurred. The id of the rule that was violated in the current rules table, and the quintuplet that identifies the faulty packet. This trap will not be sent at intervals smaller than one minute for identical information in the varbinds list variables.
avayaG350	68	IntUnAuthorizedAccessEvent			An attempt has been made to logon to the device with an invalid userid/password.
avayaG350	70	ipArpViolationTrap			

Table 4: G250/G350 Traps and Resolutions *3 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	1	avEntFanFlt	Temp		There is a faulty fan on the device. 1. Verify there are faults in the system. Use the Avaya G250/G350 Media Gateway CLI command show faults to display any faults on the G250/G350. 2. If there is a fan/temperature fault, check to see if the fans are working, and/or if there is sufficient space around the G250/G350 for air circulation. 3. Maintenance software monitors voltages applied to the media modules and other components of the G250/G350, and compares these to the general power supply unit (PSU) status bit. If none of these voltages are out of tolerance, but the PSU status indicates failure, this generates the fan fault, which will be indicated in the show faults command output. Replace the entire G250/G350. Fans and the PSU are not field replaceable.
avEntTraps	2	avEntFanOk	Temp	Notification	A faulty fan has returned to normal functioning.

Table 4: G250/G350 Traps and Resolutions *4 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	4	avEnt48vPwrFlt	Supply		There is a problem with the 48V power supply. 1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250/G350. Voltage may be reduced by a short in one of the media modules or a bad power supply. 2. Systematically, remove each media module to determine if one of the media modules is responsible for reducing the voltage levels. Replace faulty media module. 3. If the alarm clears in 10-20 seconds, it most likely was a voltage spike. Do not replace the G250/G350. Use a power monitor to monitor the power line. 4. If a brown-out condition is suspected, use a power monitor to monitor the power line. 5. If the fault persists and the show voltages command continues to show the level is out of tolerance, replace the G250/G350.
avEntTraps	5	avEnt48vPwrFltOk	Supply		The problem with the 48V power supply has been corrected.
avEntTraps	7	avEnt5vPwrFlt	Supply		There is a problem with the 5V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	8	avEnt5vPwrFltOk	Supply		The problem with the 5V power supply has been corrected.
avEntTraps	10	avEnt3300mvPwrFlt	Supply		There is a problem with the 3.3V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	11	avEnt3300mvPwrFltOk	Supply		The problem with the 3.3V power supply has been corrected.
avEntTraps	13	avEnt2500mvPwrFlt	Supply		There is a problem with the 2.5V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	16	avEnt1800mvPwrFlt	Supply		There is a problem with the 1.8V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.

4 of 16

Table 4: G250/G350 Traps and Resolutions *5 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	14	avEnt2500mvPwrFltOk	Supply		The problem with the 2.5V power supply has been corrected.
avEntTraps	17	avEnt1800mvPwrFltOk	Supply		The problem with the 1.8V power supply has been corrected.
avEntTraps	19	avEnt1600mvPwrFlt	Supply		There is a problem with the 1.6V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	20	avEnt1600mvPwrFltOk	Supply		The problem with the 1.6V power supply has been corrected.
avEntTraps	22	avEntAmbientHiThresholdTempFlt	Temp		The ambient temperature in the device is above the acceptable temperature range. 1. Verify there are faults in the system. Use the Avaya G250/G350 Media Gateway CLI command show faults to display any faults on the G250/G350. 2. If there is a temperature fault, turn off the G250/G350 and allow it to cool. 3. Reboot the G250/G350. Check to see if the fans are working and/or if there is sufficient space around the G250/G350 for air circulation. Use the CLI show faults command to check for fan problems. 4. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the media modules or a bad power supply. If there are no fan faults, use the CLI command show voltages to display voltages applied to components on the motherboard and to the media modules. 5. If the media module voltage is out of tolerance, systematically, remove each media module to determine if one of the media modules is responsible for reducing the voltage level. If one is found, replace the media module. If no media module is found to be bad, the power supply is suspect. Replace the G250/G350.
avEntTraps	23	avEntAmbientHiThresholdTempOk	Temp		The ambient temperature in the device has returned to the acceptable range.

Table 4: G250/G350 Traps and Resolutions *6 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	24	avEntAmbientLoThresholdTempFlt	Temp		The ambient temperature in the device is below the acceptable temperature range.
avEntTraps	25	avEntAmbientLoThresholdTempOk	Temp		The ambient temperature in the device has returned to the acceptable range.
					6 of 16

Table 4: G250/G350 Traps and Resolutions *7 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	30	cmgSyncSignalFault		Major	The synchronization signal has been lost. Check that the provisioned clock-sync source has a good signal using the Media Gateway CLI command show sync timing. To set synchronization timing sources on E1/T1 MM or MM710: 1. If the E1/T1 MM has not been added properly on the server, you must use the SAT command ADD DS1 before using the Media Gateway CLI commands set sync interface or set sync source. 2. Specify the primary and secondary clock sources for synchronizing the E1/T1 span, using the CLI command set synch interface. Note: The local clock is “built-in” and not provisionable. 3. Use a set sync source command to set to the specific MM710 E1/T1 media module to be used as the active clock reference. 4. Use a show sync timing command to ensure that the source is provisioned and active, or visually inspect the Yellow LED on the MM710 media module. Note: When the Yellow LED is on 2.7 seconds and off 0.3 seconds, this means the tone-clock synchronizer is in “active” mode, and an external synchronization source is being used as a synchronization reference. Setting the sync timing was successful. When the Yellow LED is on 0.3 seconds and off 2.7 seconds, this means the tone-clock synchronizer is in “active” mode and the internal (on-board) clock is being used as a synchronization reference. Setting the sync timing was not successful. 5. If there is more than one MM710 media module, and they have been set up as primary and secondary, this behavior could be on the second and not the timing of the bus.
cmgTrapTypes	31	cmgSyncSignalClear			The synchronization signal has been regained.

Table 4: G250/G350 Traps and Resolutions *8 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	32	cmgVoipHardwareFault		Major	A DSP complex serving the VoIP engines has failed.
cmgTrapTypes	33	cmgVoipHardwareClear			The DSP complex serving the VoIP engines has returned to normal functioning.
cmgTrapTypes	34	cmgSyncSignalWarn			
cmgTrapTypes	35	cmgSyncWarnClear			
cmgTrapTypes	36	cmgSyncSignalExcess			
cmgTrapTypes	37	cmgSyncExcessClear			
cmgTrapTypes	50	cmgModuleRemove			A media module has been removed.
cmgTrapTypes	52	cmgModuleInsertFault			The insertion sequence for a media module has failed.
cmgTrapTypes	53	cmgModuleInsertSuccess			A media module has been inserted.
cmgTrapTypes	57	cmgDataModuleAwohConflict			
cmgTrapTypes	71	cmgFirmwareDownloadSuccess			The Media Gateway successfully downloaded a software or configuration file.
cmgTrapTypes	73	cmgRegistrationSuccess			The Media Gateway has successfully registered with a Media Controller.
cmgTrapTypes	74	cmgMgManualReset			The Media Gateway is beginning a user-requested reset operation.
cmgTrapTypes	75	cmgModuleManualReset			A media module is beginning a user-requested reset operation.

8 of 16

Table 4: G250/G350 Traps and Resolutions *9 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	90	cmgMemoryFault		Major	The Media Gateway has detected a low memory condition. This occurs when a software module is unable to allocate memory, or the available memory falls below 4 MB. 1. Check the Media Gateway and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 2. If this trap occurs infrequently and is automatically cleared, the trap may be due to an unusual transient condition. Monitor future traps. 3. If this trap occurs frequently and is automatically cleared, it is likely that the Media Gateway software has the wrong limits set for its memory monitoring. These limits are hard coded in the software. Speak to an Avaya technical professional. 4. If this trap occurs and does not clear, the Media Gateway may be functionally impaired. Do not reset the Media Gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis. 5. If this trap occurs and the Media Gateway Processor automatically resets, then a severe processor memory shortage occurred. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
cmgTrapTypes	91	cmgMemoryClear			The low memory condition has been cleared. This occurs when the available memory rises above 5 MB.

Table 4: G250/G350 Traps and Resolutions *10 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	94	cmgFirmwareDownloadFault		Major	An attempt to download a software module has failed. 1. Check the event log to find the specific error. 2. Troubleshoot the specific error according to the information found. For example, if the string “File not found” appears in the log, then verify that the image file: a. Exists b. Has the correct name c. Resides in the correct directory
cmgTrapTypes	98	cmgIccMissingFault		Major	An internal communications controller (S8300), expected in slot 1, is missing.
cmgTrapTypes	99	cmgIccMissingClear			A missing internal communications controller (S8300) has been found.
cmgTrapTypes	100	cmgIccAutoReset		Major	The Media Gateway automatically reset the internal communications controller.
cmgTrapTypes	101	cmgIccAutoResetClear			
cmgTrapTypes	102	cmgPrimaryControllerFault		Major	The Media Gateway cannot contact the first controller in its controller list. 1. Verify that the controller list is correct. From the CLI, use the command show mgc list. The IP address should match the server or the server IP addresses. 2. If needed, correct this in configure mode in the CLI. Clear the mgc list first with the clear mgc list command. Then use a set mgc list with the correct IP addresses. 3. Verify that the primary controller is up. 4. If so, shut down every LSP
cmgTrapTypes	103	cmgPrimaryControllerClear			

Table 4: G250/G350 Traps and Resolutions *11 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	104	cmgNoControllerFault		Major	The Media Gateway does not have any controllers in its controller list. 1. Verify that the controller list is empty. From the CLI, use the command show mgc list to verify that there are no controllers listed. 2. If none are listed, correct this by adding the correct IP address of the primary server. In the CLI's 'configure' mode, use a set mgc list command with the correct IP address.
cmgTrapTypes	105	cmgnoControllerClear			The cmgNoControllerFault trap has been cleared.
cmgTrapTypes	106	cmgRegistrationFault		Major	The Media Gateway cannot register with any controllers in its controller list. 1. Verify that the controller list is correct. From the CLI, use the command show mgc list. The IP address should match the server CLAN or the server IP addresses. 2. If needed, correct this in the CLI's 'configure' mode. Clear the mgc list with the clear mgc list command. Then use a set mgc list with the correct IP addresses. 3. If the IP address in the mgc list matches the server CLAN or the server IP addresses, there may be a network problem. 4. Verify that the primary controller is up.

Table 4: G250/G350 Traps and Resolutions *12 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	108	cmgH248LinkDown		Minor	An H.248 link between the Media Gateway and its controller is down. 1. Check the server. If down, bring up. 2. If not, check the G250/G350 administration. *Since the following command causes a brief service outage, it should only be executed at the customer's convenience.* 3. If the administration is correct, reboot the G250/G350. 4. If the problem persists, check network connectivity. Use ping or traceroute to the server to check connectivity. 5. If the problem persists, speak to an Avaya technical professional.
cmgTrapTypes	109	cmgH248LinkUp			An H.248 link between the Media Gateway and its controller that was down has come back up.

Table 4: G250/G350 Traps and Resolutions *13 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	114	cmgMgAutoReset		Warning	The Media Gateway automatically reset. This may be due to a critical error from which the Media Gateway could not recover. It may be due to a maintenance test running on the call controller. It may also be due to the Media Gateway's reregistration with a call controller after being out of contact for too long. 1. Check to see if a maintenance test that resets the processor was run. 2. Check to see if the reset was due to the link with the call controller going down. If so, follow call controller link failure troubleshooting procedures. 3. Check the Media Gateway and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 4. If this trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps. 5. If this trap occurs and the Media Gateway is frequently resetting, manually reset the media gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis. 6. If this trap occurs frequently and the Media Gateway is not resetting, the Media Gateway may be functionally impaired, and is not capable of resetting itself to restore service. If service is impaired, reset the Media Gateway manually. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

Table 4: G250/G350 Traps and Resolutions *14 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	116	cmgModuleAutoReste		Warning	cmgModuleAutoReset — A media module in the Media Gateway automatically reset (rebooted). To resolve the problem, take the following steps: 1. Check if a maintenance test that resets the media module was run. 2. Check the media module and insure that it has the latest version of firmware installed. If not, install the latest version of firmware and continue to monitor. 3. If this trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps. 4. If this trap occurs and the media module does not return to service, or if this trap occurs frequently, attempt to reset the failing module from the SAT or CLI and see if this returns it to stable service. 5. If manually resetting the media module does not return it to service, and if a spare media module of the same time is available, replace the failing media module with the spare and see if the spare media module goes into service. If so, follow procedures for dealing with the original bad media module. 6. If the spare media module fails to go into service, it is possible that the spare media module is also bad. If not, manually reset the Media Gateway at a time convenient to the customer. If this restores service, both the original and the spare media modules can be considered okay. The problem is probably with the Media Gateway itself. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
cmgTrapTypes	117	cmgModuleAutoResetClear			
cmgTrapTypes	118	cmgModulePostFault		Minor	A media module failed its power-on start-up test.

Table 4: G250/G350 Traps and Resolutions *15 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	119	cmgModulePostClear			
cmgTrapTypes	122	cmgConfigUpoadFault		Major	An attempt to upload a configuration file failed. 1. Check the event log for an error message during the backup/restore process. 2. Troubleshoot the specific error according to the information found. 3. Retry the upload (backup) command; for example: copy startup-config tftp <filename> <ip address> CAUTION: Since the following command causes a brief service outage, it should only be executed at the customer's convenience. 4. If the problem persists, reboot the G250/G350.
cmgTrapTypes	124	cmgVoipOccFault			
cmgTrapTypes	125	cmgVoipOccClear			
cmgTrapTypes	126	cmgVoipAvgOccFault			
cmgTrapTypes	127	cmgVoipAvgOccClear			

Table 4: G250/G350 Traps and Resolutions *16 of 16*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	128	cmgVoipAutoReset		Warning	The VoIP module in the Media Gateway automatically reset.To resolve the problem, take the following steps: 1. Check if a maintenance test that resets the VoIP module was run. 2. Check to see if the VoIP module had its IP address re-administered. 3. Check to see if the IP address administered on the VoIP module is correct. 4. Check to see if the IP address of the Media Gateway itself can be pinged. Physical or logical connectivity issues (cabling or routing problems) in the data network can cause ping failures. 5. Check the VoIP module and insure that it has the latest version of firmware installed. If not, install the latest version of firmware and continue to monitor. 6. If this trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps. 7. If this trap occurs and the VoIP module does not return to service, or if this trap occurs frequently, attempt to reset the failing module from the SAT or CLI. 8. Manually reset the Media Gateway at a time convenient to the customer. If this restores service, the problem is probably with the Media Gateway itself. Capture the trap information. If possible, capture the event logs, using the show event-log CLI command, for analysis. Escalate. 9. If none of this works, capture the trap information. If possible, capture the event logs, using the show event-log CLI command, for analysis. Escalate.
cmgTrapTypes	129	cmgVoipAutoResetClear			

16 of 16

G450/G700 Traps

Configure the G450/G700 to send SNMP traps

Configuring the G450/G700 Media Gateway to send SNMP traps to the primary server can be accomplished by two commands:

- Layer 2 Switching Processor CLI command: **`set snmp community trap [`*`community string`*`]`**
- Media Gateway Processor (MGP) CLI command: **`set snmp trap <`*`IP address`*`> enable`**

Configure an SNMP community string for traps

SNMP requires community strings to be used for each SNMP "request". Only three community strings can be set — one each for read requests, write requests, and traps. The command for traps is **`set snmp community trap [`*`community string`*`]`**.

To configure an SNMP community string for traps

1. Open the Run dialog box.
2. Enter **`telnet <`*`IP address of L2 Processor`*`>`**
3. Log in as **root**.
4. At the L2 Processor CLI prompt, enter **`set snmp community trap [`*`community string`*`]`**
5. Enter **exit**

Configure the destination for G450/G700 SNMP traps

Events occurring on the G450/G700 cause SNMP traps to be generated. The MGP can be configured to send SNMP traps to any network management system (NMS) in the network, including the primary server. The MGP CLI **`set snmp trap`** command is the way to configure the NMS network element that will receive those traps. The traps are sent in User Datagram Protocol (UDP) on the customer's IP network.

The command syntax is:

set SNMP trap <***IP address***> *{***enable**|**disable***}*
[{all|*power*|*temp*|*app*|*module*|*config*|*voice*|*operations}]*

where **<*IP address*>** is the IP address of the NMS trap receiver that will be receiving the traps from the G450/G700, and

[{**all|power|temp|app|module|config|voice|operations*****}]*** indicates the groups whose traps will be sent to the specified receiver. If no keywords follow the IP address entry, then all traps will be enabled for the specified receiver.

If "enable" or "disable" is used without a trap designation keyword, then all traps is assumed. Up to ten trap receivers can be configured.

To configure the destination for media gateway SNMP traps

1. From the L2 Processor CLI, enter **session mgp**
2. At the **mg-xxx-n(super-user)** prompt, enter **configure**
3. At the **mg-xxx-n(configure)** prompt, enter **set snmp trap <*IP address*> enable**
4. Enter **exit**

Media Gateway Traps and Resolutions

Although alarms can be viewed from the primary server, they are normally resolved from within the media gateway. The media gateway generates the following traps. Follow the error

resolution procedures in Table 5: Media Gateway Traps and Resolutions to resolve errors indicated by these traps.

Table 5: Media Gateway Traps and Resolutions *1 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
1	2	WRN	cmgMultipleFanFault — At least two media gateway fans have been operating at less than 90% of their nominal speed for 5 minutes or more. This may be an early warning of overheating. 1. Verify there are faults in the system. Use the Media Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the media gateway. Check for voltage alarms first. If it is a voltage alarm, fix the voltage alarm. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the media modules or there may be a bad power supply. Systematically remove each media module to determine if one of the media modules is responsible for reducing the voltage levels. 2. If there is a fan/temperature fault, check to see if the fans are working, and/or if there is sufficient space around the media gateway for air circulation. 3. If none of the voltages are out of tolerance, but the PSU status indicates failure, replace the entire media gateway. Fans and the PSU are not field replaceable.
1	3	WRN	cmgMultipleFanClear - at least three fans are operating normally. The system should be operable indefinitely without overheating.

Table 5: Media Gateway Traps and Resolutions *2 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
2	4	MIN	cmgPsuFanBriefFault — The power supply fan has been operating at less than 90% of its optimal speed for 10 minutes or more, but less than 15 minutes. This may be an early warning of overheating. 1. Verify there are faults in the system. Use the Media Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the media gateway. Check for voltage alarms first. If it is a voltage alarm, fix the voltage alarm. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the media modules or there may be a bad power supply. Systematically remove each media module to determine if one of the media modules is responsible for reducing the voltage levels. 2. If there is a fan/temperature fault, check to see if the fans are working, and/or if there is sufficient space around the media gateway for air circulation. 3. If none of the voltages are out of tolerance, but the PSU status indicates failure, replace the entire media gateway. Fans and the PSU are not field replaceable.
2	5	MIN	cmgPsuFanBriefClear - The power supply fan is operating normally.
			2 of 22

Table 5: Media Gateway Traps and Resolutions *3 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
3	6	MIN	cmgPsuFanProlongedFault — The power supply fan has been operating at less than 90% of its optimal speed for 15 minutes or more. This may be an early warning of overheating. 1. Verify there are faults in the system. Use the Media Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the media gateway. Check for voltage alarms first. If it is a voltage alarm, fix the voltage alarm. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the media modules or there may be a bad power supply. Systematically remove each media module to determine if one of the media modules is responsible for reducing the voltage levels. 2. If there is a fan/temperature fault, check to see if the fans are working, and/or if there is sufficient space around the media gateway for air circulation. 3. If none of the voltages are out of tolerance, but the PSU status indicates failure, replace the entire media gateway. Fans and the PSU are not field replaceable.
3	7	MIN	cmgPsuFanProlongedClear - The power supply fan is operating normally.
	8 - 9		Reserved
			3 of 22

Table 5: Media Gateway Traps and Resolutions *4 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
4	10	MIN	cmgCpuTempWarningFault — The temperature sensor at the CPU has exceeded its warning threshold. 1. Verify there are faults in the system. Use the Media Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the media gateway. 2. If there is a temperature fault, turn off the media gateway and allow it to cool. 3. Reboot the media gateway. Check to see if the fans are working and/or if there is sufficient space around the media gateway for air circulation. Use the MGP CLI **`show faults`** command to check for fan problems. 4. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the Media Modules or a bad power supply. If there are no fan faults, use the MGP CLI command **`show voltages`** to display voltages applied to components on the motherboard and to the Media Modules. 5. If the Media Module voltage is out of tolerance, systematically, remove each Media Module to determine if one of the Media Modules is responsible for reducing the voltage level. If one is found, replace the Media Module. 6. If no Media Module is found to be bad, the power supply is suspect. Replace the media gateway.
4	11	MIN	cmgCpuTempWarningClear - The temperature sensor at the CPU has dropped below its warning threshold.

4 of 22

Table 5: Media Gateway Traps and Resolutions *5 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
5	12	MIN	cmgDspTempWarningFault — The temperature sensor at the DSP complex has exceeded its warning threshold. 1. Verify there are faults in the system. Use the Media Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the media gateway. 2. If there is a temperature fault, turn off the media gateway and allow it to cool. 3. Reboot the media gateway. Check to see if the fans are working and/or if there is sufficient space around the media gateway for air circulation. 4. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the Media Modules or a bad power supply. If there are no fan faults, use the MGP CLI command **`show voltages`** to display voltages applied to components on the motherboard and to the Media Modules. 5. If the Media Module voltage is out of tolerance, systematically, remove each Media Module to determine if one of the Media Modules is responsible for reducing the voltage level. If one is found, replace the Media Module. 6. If no Media Module is found to be bad, the power supply is suspect. Replace the media gateway.
5	13	MIN	cmgDspTempWarningClear - The temperature sensor at the DSP complex has dropped below its warning threshold.
6	14	MAJ	cmgTempShutdownFault — The CPU temperature sensor has exceeded its shutdown threshold. The system is about to begin controlled shutdown. 1. Turn off the media gateway and allow it to cool. 2. Check the fans and replace the media gateway as necessary. Fans are not field-replaceable.
6	15		Reserved
			5 of 22

Table 5: Media Gateway Traps and Resolutions *6 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
7	16	MAJ	cmgMgpPowerFault — The voltage reading at the +5.1V power source serving the media gateway processor is out of tolerance. 1. Replace the power supply only if the problem is persistent. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.
7	17	MAJ	cmgMgpPowerClear - The voltage reading at the +5.1V power source serving the media gateway processor is back within its tolerance range.
8	18	MAJ	cmgMediaModulePowerFault — The voltage reading at the -48V power source serving the media modules is out of tolerance. 1. Replace the power supply only if the problem is persistent. do not replace the power supply if there is a suspected voltage spike or temporary brown-out.
8	19	MAJ	cmgMediaModulePowerClear - The voltage reading at the -48V power source serving the media modules is back within its tolerance range.
9	20	MAJ	cmgVoipPowerFault — The voltage reading at the +3.4V power source serving the VoIP complexes is out of tolerance. 1. Replace the power supply only if the problem is persistent. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.
9	21	MAJ	cmgVoipPowerClear - The voltage reading at the +3.4V power source serving the VoIP complexes is back within its tolerance range.
10	22	MAJ	cmgDspPowerFault — The voltage reading at the +1.58V power source serving the DSP units is out of tolerance. 1. Replace the power supply only if the problem is persistent. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.
10	23	MAJ	cmgDspPowerClear - The voltage reading at the +1.58V power source serving the DSP units is back within its tolerance range.
			6 of 22

Table 5: Media Gateway Traps and Resolutions *7 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
11	24	MAJ	cmg8260PowerFault — The voltage reading at the +2.5V power source serving the 8260 processor is out of tolerance. 1. Replace the power supply only if the problem is persistent. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.
11	25	MAJ	cmg8260PowerClear - The voltage reading at the +2.5V power source serving the 8260 processor is back within its tolerance range.
12	26	MAJ	cmgAuxPowerFault - The voltage reading at the -48V auxiliary power source serving the end points is out of tolerance. 1. No action is required.
12	27	MAJ	cmgAuxPowerClear - The voltage reading at the -48V auxiliary power source serving the end points is back within its tolerance range
13	28	MAJ	cmgFanPowerFault - The voltage reading at the +12V auxiliary power source serving the fans is out of tolerance. 1. Replace the power supply only if the problem is persistent. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.
13	29	MAJ	cmgFanPowerClear - The voltage reading at the +12V auxiliary power source serving the fans has returned to within its tolerance range.

Table 5: Media Gateway Traps and Resolutions *8 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
14	30	MAJ	cmgSyncSignalFault — Synchronization signal lost. 1. Check that the provisioned clock-sync source has a good signal by entering the Media Gateway Processor (MGP) Command Line Interface (CLI) command **`show sync timing`** Procedure for setting synchronization timing sources on E1/T1 MM or MM710: 1. Be sure that the E1/T1 MM has been added properly on the server, otherwise, using the System Access Terminal (SAT), enter the **`add DS1`** command before using the MGP CLI and entering a **`set sync interface`** or **`set sync source`** command. Otherwise, the MGP CLI will not allow these commands to be executed. 2. Using the MGP's CLI, first specify the primary and secondary clock sources for synchronizing the E1/T1 span with the **`set synch interface`** command. Note: The internal clock source is not specified from the CLI - only the primary and secondary. The local clock is "built-in" and not administrable. 3. Enter a **`set sync source`** command to set to the specific MM710 E1/T1 Media Module to be used as the active clock reference. 4. Verify whether or not these commands were executed by entering **`show sync timing`** to ensure that the source is provisioned and active, or visually inspect the Yellow LED on the MM710 Media Module. Note: When the Yellow LED is on 2.7 seconds and off 0.3 seconds, this means the tone-clock synchronizer is in "active" mode, and an external synchronization source is being used as a synchronization reference. Setting the sync timing was successful. When the Yellow LED is on 0.3 seconds and off 2.7 seconds, this means the tone-clock synchronizer is in "active" mode and the internal (on-board) clock is being used as a synchronization reference. Setting the sync timing was not successful.

Table 5: Media Gateway Traps and Resolutions *9 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
14 (cont'd)	30	MAJ	5. Verify whether or not these commands were executed by entering **`show sync timing`** to ensure that the source is provisioned and active, or visually inspect the Yellow LED on the MM710 Media Module. Note: When the Yellow LED is on 2.7 seconds and off 0.3 seconds, this means the tone-clock synchronizer is in "active" mode, and an external synchronization source is being used as a synchronization reference. Setting the sync timing was successful. When the Yellow LED is on 0.3 seconds and off 2.7 seconds, this means the tone-clock synchronizer is in "active" mode and the internal (on-board) clock is being used as a synchronization reference. Setting the sync timing was not successful. 6. If there is more than one MM710 Media Module, and they have been set up as primary and secondary, this behavior could be on the second and not the timing of the bus. For more details, please consult the maintenance documentation under LEDs and E1/T1 Media Module, or see http://support.avaya.com/elmodocs2/S8300/cd/index.htm
14	31	MAJ	cmgSyncSignalClear - Synchronization signal normal.
15	32	MAJ	cmgVoipHardwareFault — One or more of the DSP complexes serving the VoIP engines has failed. 1. Check the IP configuration. 2. Reset or replace the Media Module.
15	33	MAJ	cmgVoipHardwareClear - All of the DSP complexes serving the VoIP engines are back in service.
	34 - 49		Reserved
	50		cmgModuleRemove - A media modules has been removed.
	51		Reserved
16	52	MAJ	cmgModuleInsertFault — Media module insertion sequence has failed. 1. Reset or replace the media module.

Table 5: Media Gateway Traps and Resolutions *10 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
	53		cmgModuleInsertSuccess - A media module has been inserted.
	54		cmgMgBusyout - An administrator has moved a media module or port to the busy-out state.
	55		cmgMgRelease — An administrator has moved a media module or port from the busy-out state back into service.
	56 – 69		Reserved
	70		cmgFirmwareDownloadBegun - The media gateway has begun download of a software module.
	71		cmgFirmwareDownloadSuccess - The media gateway has completed successful download of a software module.
	72		Reserved
	73		cmgRegistrationSuccess - The media gateway has successfully registered with a controller.
	74		cmgMgManualReset - The media gateway is beginning a user-requested reset operation.
	75		cmgModuleManualReset - A media module is beginning a user-requested reset operation.
	76		cmgVoipManualReset - A VoIP engine is beginning a user-requested reset operation.
	77		cmgDsuManualReset - An E1/T1 DSU is beginning a user-requested reset operation.
	78		cmgConfigUploadBegun — The Media Gateway has begun upload of a configuration file.
	79		cmgConfigUploadSuccess — The Media Gateway has completed successful upload of a configuration file.
	80 - 89		Reserved

10 of 22

Table 5: Media Gateway Traps and Resolutions *11 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
17	90	MAJ	cmgMemoryFault — The Media Gateway Processor has detected a low processor memory condition. 1. Check the Media Gateway Processor and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 2. If this trap occurs infrequently and is automatically cleared, the trap may be due to an unusual transient condition. Monitor future traps. 3. If this trap occurs frequently and is automatically cleared, it is likely that the Media Gateway Processor software has the wrong limits set for its memory monitoring. These limits are hard coded in the software. Escalate the problem. 4. If this trap occurs and does not clear, the Media Gateway may be functionally impaired. Do not reset the Media Gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis. 5. If this trap occurs and the Media Gateway Processor automatically resets, then a severe processor memory shortage occurred. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
17	91	MAJ	cmgMemoryClear - The main processor memory has returned to normal operation.
18	92	MAJ	cmgDhcpRequestFault — The Media Gateway cannot contact its DHCP server or the server failed to respond to a request. 1. Correct the DHCP problem, or correct the media gateway configuration file.
18	93	MAJ	cmgDhcpRequestClear - The media gateway received a successful response to a DHCP request.

11 of 22

Table 5: Media Gateway Traps and Resolutions *12 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
19	94	MAJ	cmgFirmwareDownloadFault — An attempt to download a software module has failed. 1. Check the event log to find the specific error. 2. Troubleshoot the specific error according to the information found. For example, if “File not found” appears in the log, then verify that the image file: a. Exists b. Has the correct name c. Resides in the correct directory 3. If the error cannot be resolved after following the above procedure, reboot the media gateway.
19	95		Reserved
20	96	WRN	cmgProcessRestartFault — a software process on the Media Gateway Processor failed. The Media Gateway Processor will attempt to restart the failed process. A successful restart of the process will clear this trap 1. Check the Media Gateway Processor and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 2. If this trap occurs infrequently and is automatically cleared, the trap may be due to an unusual transient condition. Monitor future traps. 3. If the trap occurs frequently and is automatically cleared, it may indicate an issue with a particular software module. Reset the Media Gateway at a time convenient with the customer. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis. 4. If the trap occurs and does not clear, the Media Gateway may be functionally impaired. Reset the Media Gateway at a time convenient with the customer and consistent with the impairment. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

12 of 22

Table 5: Media Gateway Traps and Resolutions *13 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
20	97	WRN	cmgProcessRestartClear - Media gateway software processes are running normally.
21	98	MAJ	cmgIccMissingFault — An internal communications controller, expected in Slot 1, is missing. 1. Check for the presence of an S8300. 2. If present, check the media gateway administration. 3. If the administration is correct, suspect the S8300.
21	99	MAJ	cmgIccMissingClear - The Internal Communications Controller expected in slot 1 is present.
22	100	MAJ	cmgIccAutoReset — The Media Gateway automatically reset the Internal Communications Controller. 1. If the problem persists, escalate.
22	101	MAJ	cmgIccAutoResetClear - The Internal Communications Controller is running normally.
23	102	MAJ	cmgPrimaryControllerFault — The Media Gateway cannot contact the first controller in its controller list. 1. Verify that the controller list is correct. From the MGP CLI, enter the command **`show mgc list`**. The IP address should match the S8700-series Server C-LAN or the S8300 Server IP address. If the IP addresses match, go to step 3. 2. If needed, correct this in 'configure' mode on the MGP's CLI by clearing the mgc list first with the **`clear mgc list`** command, and then enter **`set mgc list`** with the correct IP addresses. 3. Verify that the primary controller is up. 4. If so, shut down every LSP.
23	103	MAJ	cmgPrimaryControllerClear - The media gateway successfully contacted the first controller in its controller list.

13 of 22

Table 5: Media Gateway Traps and Resolutions *14 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
24	104	MAJ	cmgNoControllerFault — The Media Gateway cannot contact any controller in its controller list. 1. Verify that the controller list is empty. From the MGP CLI, enter the command **`show mgc list`** to verify that there are no controllers listed. 2. If none are listed, add the correct IP address of the S8700-series server or S8300. In 'configure' mode on the MGP's CLI, enter **`set mgc list`** with the correct IP address.
24	105	MAJ	cmgNoControllerClear - The media gateway successfully contacted one of the controllers in its controller list.
25	106	MAJ	cmgRegistrationFault — The Media Gateway cannot register with any controllers in its controller list. 1. Verify that the controller list is correct. From the MGP CLI, enter the command **`show mgc list`**. The IP address should match the S8700-series Server C-LAN or the S8300 Server IP addresses. 2. If needed, correct this in 'configure' mode on the MGP's CLI by clearing the mgc list with **`clear mgc list`**, then entering **`set mgc list`** with the correct IP addresses. 3. If the IP address in the mgc list matches the S8700-series Server C-LAN or the S8300 Server IP addresses, there may be a network problem. 4. Verify that the primary controller is up. 5. If the above steps do not fix the problem, reboot the media gateway.
25	107		Reserved
			14 of 22

Table 5: Media Gateway Traps and Resolutions *15 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
26	108	MIN	cmgH248LinkDown — The H.248 link between the Media Gateway and its controller is down. 1. Check the S8300 or S8700-series server. 2. If it is down, bring it up. 3. If it is **not**, check the media gateway administration. Since the following command causes a brief service outage, it should only be executed at the customer's convenience. 4. If the administration is correct, reboot the media gateway. 5. If the problem persists, check network connectivity. Use **`ping`** or **`traceroute`** to the S8700-series server or S8300 to check connectivity. 6. If the problem persists, escalate.
26	109	MIN	cmgH248LinkUp - The H.248 link between the media gateway and its controller is back in service.
27	110	MIN	cmgTestFault - Maintenance tests have failed. 1. Refer to the specific maintenance object failure for diagnosis.
27	111	MIN	cmgTestClear - Previously failed maintenance tests have passed.
28	112	MAJ	cmgTestThresholdFault - The maintenance test failure count has exceeded its reporting threshold. No action is required.
28	113	MAJ	cmgTestThresholdClear - The maintenance test failure count has dropped below its reporting threshold.

15 of 22

Table 5: Media Gateway Traps and Resolutions *16 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
29	114	WRN	cmgMgAutoReset — The Media Gateway Processor automatically reset (rebooted). The processor automatically resets when a critical error occurs from which it cannot recover. The error may be software or hardware related. It may automatically reset when it reregisters with a call controller after being out of touch for too long. This trap is generated as the Media Gateway Processor comes back up after resetting. If the Media Gateway Processor resets and fails to come back up, this trap will not be generated. 1. Check to see if a maintenance test that is supposed to reset the processor was run. 2. Check that the reset was not due to the link with the call controlling going down. If the reset is due to a link failure with the call controller, follow call controller link failure troubleshooting procedures. 3. Check the Media Gateway Processor and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 4. If this trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps. 5. If this trap occurs and the Media Gateway Processor is frequently resetting, manually reset the media gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis. 6. If this trap occurs frequently and the Media Gateway Processor is not resetting, the Media Gateway may be functionally impaired and is not capable of resetting itself to restore service. If service is impaired, reset the Media Gateway manually. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
29	115		Reserved
			16 of 22

Table 5: Media Gateway Traps and Resolutions *17 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
30	116	WRN	cmgModuleAutoReset — A Media Module in the Media Gateway automatically reset (rebooted). A Media Module automatically resets when it fails a sanity test performed by the Media Gateway Processor. 1. Check to see if a maintenance test that is supposed to reset the Media Module was run. 2. Check the Media Module and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 3. If this trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps. 4. If this trap occurs and the Media Module does not return to service, or if this trap occurs frequently, attempt to reset the failing module from the SAT or CLI and see if this returns it to stable service. 5. If manually resetting the Media Module does not return it to service, and if a spare Media Module of the same time is available, replace the failing Media Module with the spare and see if the spare Media Module goes into service. If so, follow procedures for dealing with the original, bad, Media Module. 6. If the spare Media Module fails to go into service, it is of course possible that the spare Media Module is bad as well. But that aside, try manually resetting the Media Gateway Processor at a time convenient to the customer and see if this restores service. If so, the both the original and the spare Media Modules can probably be considered okay, and the problem is probably with the Media Gateway Processor itself. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
30	117	WRN	cmgModuleAutoResetClear - The reset media module is operating normally.

Table 5: Media Gateway Traps and Resolutions *18 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
32	118	MIN	cmgModulePostFault — A Media Module failed its power-on start-up test. 1. Reset or replace the Media Module.
32	119	MIN	cmgModulePostClear - The media module power-on start-up test was successful.
33	120	MIN	cmgModuleParameterFault - A media module failed its parameter exchange. 1. Manually reboot the media gateway at a convenient time. 2. If the problem persists, escalate.
33	121	MIN	cmgModuleParameterClear - The media module's parameter exchange succeeded.
34	122	MAJ	cmgConfigUploadFault — An attempt to upload a configuration file failed. 1. Check the event log for an error message during the backup/ restore process. 2. Troubleshoot the specific error according to the information found. 3. Retry the upload (backup) command; for example: **`copy mgp-config tftp <filename> <ip address>`** Since the following command causes a brief service outage, it should only be executed at the customer's convenience. 4. If the problem persists, reboot the media gateway.
	123		Reserved
35	124	MIN	cmgVoipOccFault - One or more of the VoIP engines in the media gateway is over is its occupancy threshold as measured by a snapshot: (Channels In Use/Total Channels). No action is required.
35	125	MIN	cmgVoipOccClear - All of the VoIP engines in the media gateway are operating below occupancy threshold.
			18 of 22

Table 5: Media Gateway Traps and Resolutions *19 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
36	126	MIN	cmgVoipAvgOccFault - One or more of the VoIP engines in the media gateway is operating above its average occupancy threshold. No action is required.
36	127	MIN	cmgVoipAvgOccClear - All of the VoIP engines in the media gateway are operating below occupancy threshold.
37	128	WRN	cmgVoipAutoReset — A VoIP (Voice Over IP) module in the Media Gateway automatically reset (rebooted). A VoIP module automatically resets when it fails a sanity test performed by the Media Gateway Processor, when its IP address is administered, or when it fails a ping test performed by the Media Gateway Processor against the VoIP module's IP address. 1. Check to see if a maintenance test that is supposed to reset the VoIP module was run. 2. Check to see if the VoIP module had its IP address re-administered. 3. Check to see if the IP address administered on the VoIP module is correct. 4. Check to see if the IP address of the Media Gateway itself can be pinged. Physical or logical connectivity issues (cabling or routing problems) in the data network can cause ping failures. 5. Check the VoIP module and insure that it has the latest version of firmware installed. If it does not, install the latest version of firmware and continue to monitor. 6. If this trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps. 7. If this trap occurs and the VoIP module does not return to service, or if this trap occurs frequently, attempt to reset the failing module from the SAT or CLI and see if this returns it to stable service.

Table 5: Media Gateway Traps and Resolutions *20 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
37 (cont'd)	128	WRN	8. If manually resetting the VoIP module does not return it to service, and if a spare VoIP module of the same type is available, replace the failing VoIP module with the spare and see if the spare VoIP module goes into service. If so, follow procedures for dealing with the original, bad, VoIP module. 9. If the spare VoIP module fails to go into service, it is of course possible that the spare VoIP module is bad, as well. There may be a power issue, also. 10. Try manually resetting the Media Gateway Processor at a time convenient to the customer and see if this restores service. If so, both the original and the spare VoIP modules can probably be considered okay, and the problem is probably with the Media Gateway Processor itself. Capture the trap information. If possible, capture the event logs, using the **`show event-log`** CLI command, for analysis. Escalate. If none of this works, capture the trap information. If possible, capture the event logs, using the **`show event-log`** CLI
37	129	WRN	cmgVoipAutoResetClear - A VoIP engine has completed its automatic reset and is running normally.
39	130	MAJ	cmgDsuFpgaConfigureFault - The DSU in one of the E1/T1 media modules failed to configure its Field Programmable Gateway Array. No action is required.
39	131	MAJ	cmgDsuFpgaConfigureClear - The DSU in one of the E1/T1 media modules successfully configured its Field Programmable Gateway Array.
40	132	WRN	cmgDsuAutoReset - A DSU in one of the E1/T1 media modules began an automatic reset. No action is required.
40	133	WRN	cmgDsuAutoClear - A DSU in one of the E1/T1 media modules completed its automatic reset and is running normally.
41	134	MIN	cmgDsuDteDtrFault - One of the E1/T1 media modules has detected that the DTR signal from its DTE is off. This indicates that the DTE is not connected or not functioning.
41	135	MIN	cmgDsuDteDtrClear - One of the E1/T1 media modules has detected that the DTR signal from its DTE has returned to normal.
			20 of 22

Table 5: Media Gateway Traps and Resolutions *21 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
42	136	MIN	cmgDsuDteRtsFault - An E1/T1 media module has detected that the RTS signal from its DTE is off whenever the DTE requests to send data and during data transfer. This indicates that the DTE is not functioning.
42	137	MIN	cmgDsuDteRtsClear - An E1/T1 media module has detected that the RTS signal from its DTE has returned to normal.
43	138	MAJ	cmgDsuTxDFault - An E1/T1 media module has detected that the data received from the local DTE to be sent to the far end is either all ones or all zeroes.
43	139	MAJ	cmgDsuTxDClear - The E1/T1 media module is receiving normal data from the local DTE to be sent to the far end.
44	140	MAJ	cmgDsuRxDFailure - An E1/T1 media module has detected that the data received from the far end to be sent to the local DTE is either all ones or all zeroes.
44	141	MAJ	cmgDsuRxDClear - The E1/T1 media module is receiving normal data from the far end to be sent to the local DTE.
45	34	WRN	cmgSyncSignalWarn - A change to the port status of a board that is providing sync timing has occurred. There is only one good port out of the >1 ports configured. If this port goes out of service, trap # 30, cmgSyncSignalFault, is generated.
45	35	WRN	cmgSyncWarnClear - More than one port is in service on a board that is providing sync timing.
46	142	MIN	cmgVoipIpConfigFault - There are two possible causes: 1. Duplicate IP address 2. VoIP failed to initialize. Examine the event log to determine which failure caused the event.
46	143	MIN	cmgVoipIpConfigClear - The duplicate IP address has been changed or the VoIP reset to re-initialize.
47	144	RES	The Media Gateway is now registered to the reporting server. Alarm has been cleared.

21 of 22

Table 5: Media Gateway Traps and Resolutions *22 of 22*

Event ID	Trap #	Alarm Level	Description / Recommendation
48	145	MIN	G450/700 Media Gateway has de-registered (transient loss of registration) from the reporting server.
49	146	MAJ	G450/700 Media Gateway has unregistered (registration lost) from the reporting server. All board and call information has been cleared.
50		MAJ	G350 Media Gateway is now registered to the reporting server.
51		MIN	G350 Media Gateway has de-registered (transient loss of registration) from the reporting server.
52		MAJ	G350 Media Gateway has unregistered (registration lost) from the reporting server.
			22 of 22

G450 R2 Gateway Traps

If time slots are unavailable for announcement, G450 R2 generates two SNMP traps in the H.248 gateway to report the following:

- time slot occupancy data based on a customer-administered percentage
- time slot occupancy at 100%

G450 R2 then sends the time slot occupancy data to the CM syslog and generates a warning on FPM at 90% and 100% occupancy.

Index