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

Release 6.2
03-300430
Issue 4
July 2012

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.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). 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://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 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.

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; 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 you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 you. "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.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, 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 or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You 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 (e.g., 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). You 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").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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.

Virtualization

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. "Instance" means one unique copy of the Software. For example, if the end user customer or Business Partner would like to install 2 instances of the same type of Products, then 2 Products of that type must be ordered.

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format

US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ａ 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

This document describes the Gateway Traps for the G250, G350, G430,G450, and G700 Avaya Branch 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 Branch gateways. Serious traps trigger alarms which are communicated to an alarm management site.

Chapter 2: Alarm Format

Branch Gateways report alarms to the primary server (an S8300D,S8510, or duplicated servers) using SNMP traps. Like the alarms of the primary server, alarms from a Branch Gateway:

- Reside in the primary server 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 Branch Gateway as the maintenance object.
- 1 is the event's ID.

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

  - A specific trap (such as Trap number 3) is the SNMP mechanism to clear an alarm logged by another specific trap (in this case, Trap number 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 number is reserved for future use.
- WRN is the event's severity.
- 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 Branch Gateway Processor (MGP).
- cmgMultipleFanFault is the trap name.

Chapter 3: SNMP alarm reporting for Branch Gateways

Setting up SNMP alarm reporting involves configuring the primary server to report alarms and configuring the Branch Gateway to send SNMP traps.

Configuration of the primary server to send SNMP alarms

The primary server may be either an S8300D, S8510, and duplicated servers. The server supports two methods for reporting alarms. Either method, both, or no alarm-reporting method may be used at a given site.

Note:

The new S8800 servers do not support modem, instead report alarms to SAL gateway over LAN

- *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 System View 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.

Adding INADS phone numbers and enabling alarms to INADS

About this task

Using the primary server's Linux shell command, you can administer the dial-out modem to send alarms in the OSS method. In this example, the primary server is S8300D, and the services support agency is Avaya's Initialization and Administration System (INADS).

Before you begin

Ensure that:

- Communication Manager administration is complete.
- a USB modem is installed.
- the S8300D server is the primary controller. Use the information acquired from the ART tool. For information about the ART tool, see *Installing and Upgrading the Avaya S8300D Server*, 555-234-100 and *Installing and Upgrading the Avaya G700 Branch Gateway*, 03-603333.

Procedure

To add INADS phone numbers and enable alarms to INADS:

Procedure

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

Chapter 4: G250, G350, G430, and G450 traps

This section describes the set of traps that are defined for the Avaya G250, G350, and G450 Branch Gateway. The Avaya G250, G350, and G450 Branch Gateway uses SNMPv3 for traps and alarms.

The Dynamic Trap Manager feature of the G250, G350, G430, and G450 ensures that SNMP traps and alarms are always sent to the currently active Branch Gateway Controller. By default, the Dynamic Trap Manager sends all SNMP messages to the currently active MGC. Using the **`snmp-server dynamic-trap-manager`** CLI command, you can configure the Dynamic Trap Manager to manage only a subset of SNMP messages.

Configuring G250, G350, G430, and G450 to send SNMP alarms

About this task

Use the following procedure to configure the Avaya G250, G350, and G450 Branch Gateway to send SNMP traps to the primary server.

Procedure

1. Enable the SNMP agent.
2. Specify the SNMP host.
3. Setup SNMP authentication.

   Refer to CLI Commands on page 20 to perform these tasks using the CLI commands.

   Note:

   For dynamic trap manager, only v1/v2c traps is supported.

CLI commands

Table 1: CLI commands

Task Name	Command
Enabling the SNMP agent ip snmp-server	**ip snmp-server**
Specifying the SNMP host snmp-server host	**snmp-server host**
Creating an SNMPv3 view	**snmp-server view viewname subtree**
Creating an SNMPv3 group and specifying the views	**snmp-server group groupname read readviewname write writeviewname notify notifyviewname**
Creating a user and add the user to a group	**nmp-server user username groupname**

Host configuration for G250, G350, G430, and G450 SNMP traps

Events occurring on the G250 and G350 Branch Gateways cause SNMP traps to be generated. The Avaya G250, G350, and G450 Branch 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 and G350 Branch Gateways CLI **snmp-server host** command. The traps are sent in User Datagram Protocol (UDP) on the customer 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 SNMPv3 Notification Types on page 21 for a full list of notification types that can be configured.

SNMPv3 notification types

Table 2: SNMPv3 notification types

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
branch-gateway	Branch 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
policy	Changes in policy (L3 devices) notifications
link-faults	link down notifications
filesys	Download/upload/backup/restore events.
tftp-server	tftp server events
ipsec	IPSEC events.

Pre-configured views and groups for SNMPv3 authentication

To use SNMPv3 authentication, you must create users, groups, and views for the G250, G350 gateways.

The G250, G350 Branch Gateways provide several pre-configured views and groups for setting up SNMP authentication. Refer to Table 3 on page 22 and Table 4 on page 22 for a description of these objects and how they can be used.

Table 3: 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 4: G250, G350 pre-configured groups

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
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

Group Name	Security Model	Security Level	Read View Name	Write View Name	Trap View Name
v3AdminViewG	v3 (USM)	3 (AuthPriv)	iso	iso	iso

G250, G350, G430, and G450 traps and resolutions

Although these alarms can be viewed from the primary server, they are normally resolved from within the Avaya G250, G350, and G450 Branch Gateway. The G250, G350/G450 generates the following traps. Follow the error resolution procedures in the sections below to resolve errors indicated by these traps.

coldStart

Enterprise snmpTraps

Trap ID 1

Name coldStart

SNMP Filtering Group generic

Severity Warning

Description 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.

warmStart

Enterprise snmpTraps

Trap ID 2

Name warmStart

SNMP Filtering Group generic

Severity Warning

Description	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.

linkDown

Enterprise	snmpTrap
Trap ID	3
Name	linkDown
SNMP Filtering Group	generic
Severity	Warning
Description	There is a failure in one of the communication links in the agent's configuration.

linkUp

Enterprise	snmpTraps
Trap ID	4
Name	linkUp
SNMP Filtering Group	generic
Severity	Warning
Description	One of the communication links in the agent's configuration has come up.

authenticFailure

Enterprise	snmpTrap
Trap ID	5

Name	authenticFailure
SNMP Filtering Group	generic
Severity	Notification
Description	The protocol is not properly authenticated.

risingAlarm

Enterprise	rmonEventsV2
Trap ID	1
Name	risingAlarm
SNMP Filtering Group	rmon
Severity	Warning
Description	An alarm entry has crossed its rising threshold.

fallingAlarm

Enterprise	rmonEventsV2
Trap ID	2
Name	fallingAlarm
SNMP Filtering Group	rmon
Severity	Warning
Description	An alarm entry has crossed its falling threshold.

Procedure

frDLCIStatusChange

Enterprise	frameRelayTraps
Trap ID	1
Name	frDLCIStatusChange
SNMP Filtering Group	wan
Description	A DLCI has been created or deleted, or has state changes.

lntConfigChangeEvent

Enterprise	avayaG350
Trap ID	1
Name	lntConfigChangeEvent
Severity	Info
Description	The configuration has been changed.

deleteSWRedundancyTrap

Enterprise	lntSWRedundancyEvents
Trap ID	12
Name	deleteSWRedundancyTrap
SNMP Filtering Group	sw-redundancy
Severity	Info
Description	A redundancy link has been deleted. Only supported by G350/G450/G450.

createSWRedundancyTrap

Enterprise	avayaG350
Trap ID	13
Name	createSWRedundancyTrap
Severity	Info
Description	A redundancy link has been created for the specified ports.

duplicateIPTrap

Enterprise	avayaG350
Trap ID	27
Name	duplicateIPTrap
Severity	Warning
Description	A duplicate IP address has been identified.

wanPhysicalAlarmOn

Enterprise	avayaG350
Trap ID	30
Name	wanPhysicalAlarmOn
Severity	Critical
Description	An E1/T1 serial cable has been disconnected.

wanPhysicalAlarmOff

Enterprise	avayaG350
Trap ID	31
Name	wanPhysicalAlarmOff
Severity	Notification
Description	An E1/T1 serial cable has been reconnected.

wanLocalAlarmOn

Enterprise	avayaG350
Trap ID	32
Name	wanLocalAlarmOn
Severity	Error
Description	A local alarm (such as LOS) has been generated.

wanLocalAlarmOff

Enterprise	avayaG350
Trap ID	33
Name	wanLocalAlarmOff
Severity	Notification
Description	A local alarm (such as LOS) has been cleared.

wanRemoteAlarmOn

Enterprise	avayaG350
Trap ID	34
Name	wanRemoteAlarmOn
Severity	Error
Description	A remote alarm (such as AIS) has been generated.

wanRemoteAlarmOff

Enterprise	avayaG350
Trap ID	35
Name	wanRemoteAlarmOf
Severity	Notification
Description	A remote alarm (such as AIS) has been cleared.

wanMinorAlarmOn

Enterprise	avayaG350
Trap ID	36
Name	wanMinorAlarmOn
Severity	Warning

wanMinorAlarmOff

Enterprise	avayaG350

Trap ID	37
Name	wanMinorAlarmOff
Severity	Notification

IntPolicyChangeEvent

Enterprise	avayaG350
Trap ID	60
Name	IntPolicyChangeEvent
Severity	Info
Description	The active policy list for the specified device or module has changed.

ipPolicyAccessControlListLvlRuleTrap

Enterprise	avayaG350
Trap ID	62
Name	ipPolicyAccessControlListLvlRuleTrap
Description	A packet fragment has been denied access on the specified interface.

IntPolicyAccessControlViolationFit

Enterprise	avayaG350
Trap ID	64
Name	IntPolicyAccessControlViolationFit
Severity	Warning
Description	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.

IntUnAuthorizedAccessEvent

Enterprise avayaG350

Trap ID 68

Name IntUnAuthorizedAccessEvent

Description An attempt has been made to logon to the device with an invalid userid/ password.

ipArpViolationTrap

Enterprise avayaG350

Trap ID 70

Name ipArpViolationTrap

avEntFanFlt

Enterprise avEntTraps

Trap ID 1

Name avEntFanFlt

SNMP Filtering Group hardware

Severity error

Description An attempt has been made to logon to the device with an invalid userid or password.

Resolving the malfunctioning fan on the device

Procedure

1. Check if there are faults in the system.Use the Avaya G250, G350, and G450 Branch Gateway CLI command show faults to display any faults on the G250 and G350 Branch Gateways.
2. If there is a fan or temperature fault, check if the fans are working, and if there is sufficient space around the G250 and G350 for air circulation.
3. Maintenance software monitors voltages applied to the media modules and other components of the G250 and 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 and G350. Fans and the PSU are not field replaceable.

avEntFanOk

Enterprise	avEntTraps
Trap ID	2
Name	avEntFanOk
Severity	Notification
Description	A faulty fan has returned to normal functioning.

avEnt48vPwrFlt

Enterprise	avEntTraps
Trap ID	4
Name	avEnt48vPwrFlt
SNMP Filtering Group	hardware
Severity	Notification

Description	There is a problem with the 48V power supply.

Resolving the problem with power supply

Procedure

1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250 and G350 Branch Gateways.

   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 and G350 Branch Gateways. 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 and G350 Branch Gateways.

avEnt48vPwrFltOk

Enterprise	avEntTraps
Trap ID	5
Name	avEnt48vPwrFltOk
SNMP Filtering Group	hardware
Severity	Error
Description	The problem with the 48V power supply has been corrected.

avEnt5vPwrFlt

Enterprise	avEntTraps
Trap ID	7
Name	avEnt5vPwrFlt
SNMP Filtering Group	hardware
Severity	Error
Description	There is a problem with the 5V power supply.

Resolving the problem with power supply

Procedure

1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250 and G350 Branch Gateways.

   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 and G350 Branch Gateways. 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 and G350 Branch Gateways.

avEnt5vPwrFltOk

Enterprise	avEntTraps
Trap ID	8

Name	avEnt5vPwrFltOk
SNMP Filtering Group	hardware
Severity	Notification
Description	The problem with the 5V power supply has been corrected.

avEnt3300mvPwrFlt

Enterprise	avEntTraps
Trap ID	10
Name	avEnt3300mvPwrFlt
SNMP Filtering Group	hardware
Severity	error
Description	There is a problem with the 3.3V power supply.

Resolving the problem with power supply

Procedure

1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250 and G350 Branch Gateways.

   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 and G350 Branch Gateways. 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 and G350 Branch Gateways.

avEnt3300mvPwrFltOk

Enterprise	avEntTraps
Trap ID	11
Name	avEnt3300mvPwrFltOk
SNMP Filtering Group	hardware
Severity	Notification
Description	The problem with the 3.3V power supply has been corrected.

avEnt2500mvPwrFlt

Enterprise	avEntTraps
Trap ID	13
Name	avEnt2500mvPwrFlt
SNMP Filtering Group	hardware
Severity	Error
Description	There is a problem with the 2.5V power supply.

Resolving the problem with power supply

Procedure

1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250 and G350 Branch Gateways.

   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 and G350 Branch Gateways. 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 and G350 Branch Gateways.

avEnt1800mvPwrFlt

Enterprise	avEntTraps
Trap ID	16
Name	avEnt1800mvPwrFlt
SNMP Filtering Group	Hardware
Severity	Error
Description	There is a problem with the 1.8V power supply.

Resolving the problem with power supply

Procedure

1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250 and G350 Branch Gateways.

   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 and G350 Branch Gateways. 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 and G350 Branch Gateways.

avEnt2500mvPwrFltOk

Enterprise	avEntTraps
Trap ID	14
Name	avEnt2500mvPwrFltOk
SNMP Filtering Group	Hardware
Severity	Notification
Description	The problem with the 2.5V power supply has been corrected.

avEnt1800mvPwrFltOk

Enterprise	avEntTraps
Trap ID	17
Name	avEnt1800mvPwrFltOk
SNMP Filtering Group	Hardware
Severity	Notification
Description	The problem with the 1.8V power supply has been corrected.

avEnt1600mvPwrFlt

Enterprise	avEntTraps
Trap ID	19
Name	avEnt1600mvPwrFlt
SNMP Filtering Group	Hardware

Severity	Error
Description	There is a problem with the 1.6V power supply.

Resolving the problem with power supply

Procedure

1. Check voltages. Use the CLI command show voltages to determine voltages for media modules and other components of the G250 and G350 Branch Gateways.

   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 and G350 Branch Gateways. 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 and G350 Branch Gateways.

avEnt1600mvPwrFltOk

Enterprise	avEntTraps
Trap ID	20
Name	avEnt1600mvPwrFltOk
SNMP Filtering Group	Hardware
Severity	Notification
Description	The problem with the 1.6V power supply has been corrected.

avEntAmbientHiThresholdTempFlt

Enterprise	avEntTraps
Trap ID	22
Name	avEntAmbientHiThresholdTempFlt
SNMP Filtering Group	Hardware
Severity	Error
Description	The ambient temperature in the device is above the acceptable temperature range.

Resolving the problem with the ambient temperature in the device

Procedure

1. Verify there are faults in the system. Use the Avaya G250/G350/G450 Branch 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.
6. If no media module is found to be bad, the power supply is suspect. Replace the G250 and G350 Branch Gateways.

avEntAmbientHiThresholdTempOk

Enterprise	avEntTraps
Trap ID	23
Name	avEntAmbientHiThresholdTempFlt
SNMP Filtering Group	Hardware
Severity	Notification
Description	The ambient temperature in the device has returned to the acceptable range.

avEntAmbientLoThresholdTempFlt

Enterprise	avEntTraps
Trap ID	24
Name	avEntAmbientHiThresholdTempFlt
SNMP Filtering Group	Hardware
Severity	Error
Description	The ambient temperature in the device is below the acceptable temperature range.

avEntAmbientLoThresholdTempOk

Enterprise	avEntTraps
Trap ID	25
Name	avEntAmbientLoThresholdTempOk
SNMP Filtering Group	Hardware
Severity	Notification

Description	The ambient temperature in the device has returned to the acceptable range.

cmgSyncSignalFault

Enterprise	cmgTrapTypes
Trap ID	30
Name	cmgSyncSignalFault
SNMP Filtering Group	media-gateway
Severity	Major
Description	The synchronization signal has been lost.

Resolving the issue with the synchronization signal

Procedure

1. Check that the provisioned clock-sync source has a good signal using the Branch Gateway CLI command show sync timing.
2. To set synchronization timing sources on E1/T1 MM or MM710:
   a. If the E1/T1 MM has not been added properly on the server, you must use the SAT command ADD DS1 before using the Branch Gateway CLI commands set sync interface or set sync source.
   b. 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.
   c. Use a set sync source command to set to the specific MM710 E1/T1 media module to be used as the active clock reference.
   d. 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, the tone-clock synchronizer is in the active mode, and an external synchronization source is being used as a synchronization reference. Setting the synchronization 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.

3. 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.

cmgSyncSignalClear

Enterprise	cmgTrapTypes
Trap ID	31
Name	cmgSyncSignalClear
SNMP Filtering Group	media-gateway
Severity	Notification
Description	The synchronization signal has been regained.

cmgVoipHardwareFault

Enterprise	cmgTrapTypes
Trap ID	32
Name	cmgVoipHardwareFault
SNMP Filtering Group	media-gateway
Severity	Warning
Description	A DSP complex serving the VoIP engines has failed.

cmgVoipHardwareClear

Enterprise	cmgTrapTypes

Trap ID	33
Name	cmgVoipHardwareClear
SNMP Filtering Group	media-gateway
Severity	Warning
Description	The DSP complex serving the VoIP engines has returned to normal functioning.

cmgSyncSignalWarn

Enterprise	cmgTrapTypes
Trap ID	34
Name	cmgSyncSignalWarn
SNMP Filtering Group	media-gateway
Severity	Error
Description	Synchronization signal lost.

cmgSyncWarnClear

Enterprise	cmgTrapTypes
Trap ID	35
Name	cmgSyncWarnClear
SNMP Filtering Group	media-gateway
Severity	Notification
Description	Synchronization signal normal.

cmgSyncSignalExcess

Enterprise	cmgTrapTypes
Trap ID	36
Name	cmgSyncSignalExcess
SNMP Filtering Group	media-gateway
Severity	Error
Description	The synchronization signal source (primary or secondary) is experiencing excessive failures in a short period causing excessive switching to an alternate source.

cmgSyncExcessClear

Enterprise	cmgTrapTypes
Trap ID	37
Name	cmgSyncExcessClear
SNMP Filtering Group	media-gateway
Severity	Notification
Description	Synchronization signal source which was causing excessive switching due to excessive failures is now normal.

cmgModuleRemove

Enterprise	cmgTrapTypes
Trap ID	50
Name	cmgModuleRemove
SNMP Filtering Group	media-gateway
Severity	Notification

Description	A media module has been removed.

cmgModuleInsertFault

Enterprise	cmgTrapTypes
Trap ID	52
Name	cmgModuleInsertFault
SNMP Filtering Group	media-gateway
Severity	Alert
Description	The insertion sequence for a media module has failed.

cmgModuleInsertSuccess

Enterprise	cmgTrapTypes
Trap ID	53
Name	cmgModuleInsertSuccess
SNMP Filtering Group	media-gateway
Severity	Notification
Description	A media module has been inserted.

cmgDataModuleAwohConflict

Enterprise	cmgTrapTypes
Trap ID	57
Name	cmgDataModuleAwohConflict
SNMP Filtering Group	media-gateway
Severity	Error

Description	This event is generated when a data module is found in a slot that was Administered without hardware as a voice module in the call controller.

cmgFirmwareDownloadSuccess

Enterprise	cmgTrapTypes
Trap ID	71
Name	cmgFirmwareDownloadSuccess
SNMP Filtering Group	media-gateway
Severity	Notification
Description	The Branch Gateway successfully downloaded a software or configuration file.

cmgRegistrationSuccess

Enterprise	cmgTrapTypes
Trap ID	73
Name	cmgRegistrationSuccess
SNMP Filtering Group	media-gateway
Severity	Notification
Description	The Branch Gateway has successfully registered with a Media Controller.

cmgMgManualReset

Enterprise	cmgTrapTypes
Trap ID	74

Name	cmgMgManualReset
SNMP Filtering Group	media-gateway
Severity	Notification
Description	The Branch Gateway is beginning a user-requested reset operation.

cmgModuleManualReset

Enterprise	cmgTrapTypes
Trap ID	75
Name	cmgModuleManualReset
SNMP Filtering Group	media-gateway
Severity	Error
Description	A media module is beginning a user-requested reset operation.

cmgMemoryFault

Enterprise	cmgTrapTypes
Trap ID	90
Name	cmgMemoryFault
SNMP Filtering Group	media-gateway
Severity	Alert
Description	The Branch 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.

Resolving the problem of low memory

Procedure

1. Check the Branch Gateway and ensure that it has the latest version of firmware installed. Install the latest version of firmware and continue to monitor if not installed.
2. If the 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 is likely that the Branch 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 the trap occurs and does not clear, the Branch Gateway may be functionally impaired. Do not reset the Branch Gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
5. If the trap occurs and the Branch 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.

cmgMemoryClear

Enterprise	cmgTrapTypes
Trap ID	91
Name	cmgMemoryClear
SNMP Filtering Group	media-gateway
Severity	Notification
Description	The low memory condition has been cleared. This occurs when the available memory rises above 5 MB.

cmgFirmwareDownloadFault

Enterprise	cmgTrapTypes

Trap ID	94
Name	cmgFirmwareDownloadFault
SNMP Filtering Group	media-gateway
Severity	Error
Description	An attempt to download a software module has failed.

Downloading a software module

Procedure

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:
   - Exists
   - Has the correct name
   - Resides in the correct directory

cmgIccMissingFault

Enterprise	cmgTrapTypes
Trap ID	98
Name	cmgIccMissingFault
SNMP Filtering Group	media-gateway
Severity	Error
Description	An internal communications controller (S8300D), expected in slot 1, is missing.

cmgIccMissingClear

Enterprise	cmgTrapTypes
Trap ID	99
Name	cmgIccMissingClear
SNMP Filtering Group	media-gateway
Severity	Notification
Description	A missing internal communications controller (S8300D) has been found.

cmgIccAutoReset

Enterprise	cmgTrapTypes
Trap ID	100
Name	cmgIccAutoReset
SNMP Filtering Group	media-gateway
Severity	Error
Description	The Branch Gateway automatically reset the internal communications controller.

cmgIccAutoResetClear

Enterprise	cmgTrapTypes
Trap ID	101
Name	cmgIccAutoResetClear
SNMP Filtering Group	media-gateway
Severity	Notification

Description	The Internal Communications Controller is running normally.

cmgPrimaryControllerFault

Enterprise	cmgTrapTypes
Trap ID	102
Name	cmgPrimaryControllerFault
SNMP Filtering Group	media-gateway
Severity	Error
Description	The Branch Gateway cannot contact the first controller in its controller list.

Contacting the first controller

Procedure

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. If so, shut down every LSP.

cmgPrimaryControllerClear

Enterprise	cmgTrapTypes
Trap ID	103
Name	cmgPrimaryControllerClear
SNMP Filtering Group	media-gateway
Severity	Notification

Description	The Branch Gateway has successfully contacted the first controller in its controller list.

cmgNoControllerFault

Enterprise	cmgTrapTypes
Trap ID	104
Name	cmgNoControllerFault
SNMP Filtering Group	media-gateway
Severity	Error
Description	The Branch Gateway does not have any controllers in its controller list.

Checking the controller list

Procedure

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 'configure' mode, use a set mgc list command with the correct IP address.

cmgnoControllerClear

Enterprise	cmgTrapTypes
Trap ID	105
Name	cmgnoControllerClear
SNMP Filtering Group	media-gateway
Severity	Notification

Description	The cmgNoControllerFault trap has been cleared.

cmgRegistrationFault

Enterprise	cmgTrapTypes
Trap ID	106
Name	cmgRegistrationFault
SNMP Filtering Group	media-gateway
Severity	Error
Description	The Branch Gateway cannot register with any controllers in its controller list.

Registering controllers in the controller list

Procedure

1. Verify that the controller list is correct. From the CLI, use the command **`show mgc list`**. The IP address must match the server CLAN or the server IP addresses.
2. If needed, correct this in the CLI configure mode. Clear the mgc list with the **`clear mgc list`** command. Then, use the **`set mgc list`** command 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. Verify that the primary controller is up.

cmgRegistrationSuccess

Enterprise	cmgTrapTypes
Trap ID	107
Name	cmgRegistrationSuccess
SNMP Filtering Group	media-gateway

Severity	Notification
Description	The Branch Gateway has successfully registered with a controller.

cmgH248LinkDown

Enterprise	cmgTrapTypes
Trap ID	108
Name	cmgH248LinkDown
SNMP Filtering Group	media-gateway
Severity	Error
Description	An H.248 link between the Branch Gateway and its controller is down.

Fixing the H.248 link between the Branch Gateway and its controller

Procedure

1. Check the server power. If down, bring up. If not, check the G250 and G350 administration.

   Since the following command causes a brief service outage, it should only be executed at the customer's convenience.
2. If the administration is correct, reboot the G250 and G350 Branch Gateways.
3. If the problem persists, check network connectivity. Use **`ping`** or **`traceroute`** to the server to check connectivity.
4. If the problem persists, contact an Avaya technical professional.

cmgH248LinkUp

Enterprise	cmgTrapTypes
Trap ID	109

Name	cmgH248LinkUp
SNMP Filtering Group	media-gateway
Severity	Notification
Description	An H.248 link between the Branch Gateway and its controller that was down has been restored.

cmgMgAutoReset

Enterprise	cmgTrapTypes
Trap ID	114
Name	cmgMgAutoReset
SNMP Filtering Group	media-gateway
Severity	Error
Description	The Branch Gateway automatically reset. This may be due to a critical error from which the Branch Gateway could not recover. It may be due to a maintenance test running on the call controller. It may also be due to the Branch Gateway re-registration with a call controller after being out of contact for too long.

Resolving the automatic reset problem of the Branch Gateway

Procedure

1. Check 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 Branch Gateway and ensure 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 the trap occurs infrequently, the trap might be due to an unusual transient condition. Monitor future traps.
5. If the trap occurs and the Branch Gateway is frequently resetting, manually reset the Branch Gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

6. If the trap occurs frequently and the Branch Gateway is not resetting, the Branch Gateway may be functionally impaired, and is not capable of resetting itself to restore service. If the service is impaired, reset the Branch Gateway manually. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

cmgModuleAutoReset

Enterprise	cmgTrapTypes
Trap ID	116
Name	cmgMgAutoReset
SNMP Filtering Group	media-gateway
Severity	Error
Description	A media module in the Branch Gateway automatically reset (rebooted).

Resolving the automatic reset problem of a media module in the Branch Gateway

Procedure

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 the trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps.
4. If the trap occurs and the media module does not return to service, or if the 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 Branch 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 Branch Gateway itself. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

cmgModuleAutoResetClear

Enterprise	cmgTrapTypes
Trap ID	117
Name	cmgModuleAutoResetClear
SNMP Filtering Group	media-gateway
Severity	Notification
Description	The reset media module is running normally.

cmgModulePostFault

Enterprise	cmgTrapTypes
Trap ID	118
Name	cmgModulePostFault
SNMP Filtering Group	media-gateway
Severity	Warning
Description	A media module failed its power-on start-up test.

cmgModulePostClear

Enterprise	cmgTrapTypes
Trap ID	119
Name	cmgModulePostClear

SNMP Filtering Group	media-gateway
Severity	Notification
Description	Media module power-on startup test successful.

cmgConfigUpoadFault

Enterprise	cmgTrapTypes
Trap ID	122
Name	cmgConfigUpoadFault
SNMP Filtering Group	media-gateway
Severity	Error
Description	An attempt to upload a configuration file failed.

Uploading a configuration file

Procedure

1. Check the event log for an error message during the backup and 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 and G350 Branch Gateways.

cmgVoipOccFault

Enterprise	cmgTrapTypes

Trap ID	124
Name	cmgVoipOccFault
SNMP Filtering Group	media-gateway
Severity	Notification
Description	One or more of the VoIP engines in the Branch Gateway is over its occupancy threshold, as measured by a snapshot: (Channels In Use)/(Total Channels).

cmgVoipOccClear

Enterprise	cmgTrapTypes
Trap ID	125
Name	cmgVoipOccClear
SNMP Filtering Group	media-gateway
Severity	Informational
Description	All the VoIP engines in the Branch Gateway are operating below occupancy threshold, as measured by a snapshot: (Channels In Use) / (Total Channels).

cmgVoipAvgOccFault

Enterprise	cmgTrapTypes
Trap ID	126
Name	cmgVoipAvgOccFault
SNMP Filtering Group	media-gateway
Severity	Informational
Description	One or more of the VoIP engines in the Branch Gateway is over its average occupancy threshold.

cmgVoipAvgOccClear

Enterprise	cmgTrapTypes
Trap ID	127
Name	cmgVoipAvgOccClear
SNMP Filtering Group	media-gateway
Severity	Informational
Description	All the VoIP engines in the Branch Gateway are operating below occupancy threshold, as measured by a snapshot: (Channels In Use) / (Total Channels).

cmgVoipAutoReset

Enterprise	cmgTrapTypes
Trap ID	128
Name	cmgVoipAutoReset
SNMP Filtering Group	media-gateway
Severity	Warning
Description	The VoIP module in the Branch Gateway automatically reset.

Resolving the automatic reset problem of a VOIP module in the Branch Gateway

Procedure

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 Branch 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 ensure that it has the latest version of firmware installed. If not, install the latest version of firmware and continue to monitor.
6. If the trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps.
7. If the trap occurs and the VoIP module does not return to service, or if the trap occurs frequently, attempt to reset the failing module from the SAT or CLI.
8. Manually, reset the Branch Gateway at a time convenient to the customer. If this restores service, the problem is probably with the Branch 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.

cmgVoipAutoResetClear

Enterprise	cmgTrapTypes
Trap ID	129
Name	cmgVoipAutoResetClear
SNMP Filtering Group	media-gateway
Severity	Informational
Description	A VoIP engine has completed automatic reset, and is running normally.

G430 and G450 traps

Table 5: G430 and G450 traps

Enterprise	Trap Id	Name	SNMP filtering group	Severity	Description
avEntPhyChFru	1	avEntPhyChFruRemoval	Hardware	Minor	Removal of FRU (Expansion unit in G430), Fan Tray and Power Supply in G450.
avEntPhyChFru	2	avEntPhyChFruInsertion	Hardware	Minor	Insertion of FRU (Expansion unit in G430), Fan Tray and Power Supply in G450.
avEntPhyChFru	3	avEntPhyChFruPsuFlt	Hardware	Minor	PSU failure (G450 only).
avEntPhyChFru	4	avEntPhyChFruPsuFltOk	Hardware	Minor	PSU is OK (G450 only).
avEntPhyChFru	5	avEntPhyChFruExpansionTestFailure	Hardware	Minor	Expansion unit test failed (G430 only)
avEntPhyChFru	6	avEntPhyChFruExpansionTestClear	Hardware	Minor	Expansion test unit pass (G430 only)

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 Avaya Aura® CM syslog and generates a warning on FPM at 90% and 100% occupancy.

Chapter 5: G700 Traps

Configuration of G700 to send SNMP traps

Configuring the G700 Branch 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]`**
- Branch Gateway Processor (MGP) CLI command: **`set snmp trap`** *IP address* **`enable`**

Configuring an SNMP community string for traps

About this task

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:

Procedure

1. Open the Rundialog 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`.

Destination for G700 SNMP traps

Events occurring on the 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 traps are sent in User Datagram Protocol (UDP) on the customer 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 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 are assumed. Up to ten trap receivers can be configured.

Configuring the destination for G700 SNMP traps

About this task

To configure the destination for Branch Gateway SNMP traps:

Procedure

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`.

Chapter 6: GEM alarm rules

Most fault traps have a corresponding clear trap that indicates an error condition has ceased to exist. The alarm rules for the clear traps generate a resolved (RES) alarm, which in the future may result in the GAM and NAM notifying INADS that the alarm has been resolved and removing the alarm from its alarm list.

Important:

Event IDs pertain to a particular condition and are associated with a specific fault/clear trap pair.

After initial deployment, the event ID for a given condition should not change. Consequently, alarm rules for new traps from the respective sources should be added with new event ids.

Classification of GEM alarm rules

Alarm rules that indicate a level of MAJ or MIN will result in an alarm report sent to INADS (subject to abbreviated alarming policies).In addition, services personnel record such alarms in the GAM and NAM alarm list for examination.

Alarm rules that indicate a level of WRN will not result in an alarm being reported to INADS, but the GAM and NAM will contain an alarm record for such an alarm.

The following general principles are used in classifying the alarm level of alarms pertaining to various faults.

- If a fault would lead to failures in call processing, the condition should result in a MAJ alarm.
- If a fault would lead to decreased capacity for call processing, the condition should result in a MIN alarm.

Note:

If a fault may not lead to any impairment in call processing, the condition should result in a WRN alarm.

Alarm rules are listed for the following:

- GEM alarm rules for generic Private Avaya Enterprise gateway traps on page 68.
- GEM alarm rules for the standard traps defined by IETF MIBs on page 69
- GEM alarm rules for WAN Traps on page 70

- GEM alarm rules for clock sync and Media Module events on page 70
- GEM alarm rules for Power over Ethernet traps on page 71

GEM alarm rules for generic Private Avaya Enterprise gateway traps

These traps apply to the G350 Branch Gateway. The table has some rules that are unique to G350.

Note:

The sources of all the below rules is GW_ENV.

Table 6: Alarm rules

Device	Token 1	evntId	Level	son	type	logId	dest	Description
snmptrapd	AvEntFanFlt	1	MAJ	X	ACT	A	YY	
snmptrapd	AvEntFanOk	1	MAJ	X	RES	A	YY	
snmptrapd	AvEnt48vPwrFlt	2	MAJ	X	ACT	A	YY	
snmptrapd	AvEnt48vPwrFltOK	2	MAJ	X	RES	A	YY	
snmptrapd	AvEnt5vPwrFlt	3	MAJ	X	ACT	A	YY	
snmptrapd	AvEnt5vPwrFltOK	3	MAJ	X	RES	A	YY	
snmptrapd	AvEnt3300mvPwrFlt	4	MAJ	X	ACT	A	YY	
snmptrapd	AvEnt3300mvPwrFltOK	4	MAJ	X	RES	A	YY	
snmptrapd	AvEnt2500mvPwrFlt	5	MAJ	X	ACT	A	YY	
snmptrapd	AvEnt2500mvPwrFltOK	5	MAJ	X	RES	A	YY	Field Replaceable Unit Removal
snmptrapd	AvEnt1800mvPwrFlt	6	MAJ	X	ACT	A	YY	Field Replaceable Unit Insertion
snmptrapd	AvEnt1800mvPwrFltOK	6	MAJ	X	RES	A	YY	Power Supply Fault

Device	Token 1	evntId	Level	son	type	logId	dest	Description
snmptrapd	AvEnt1600mvPwrFlt	7	MAJ	X	ACT	A	YY	Power Supply Ok
snmptrapd	AvEnt1600mvPwrFltOK	7	MAJ	X	RES	A	YY	
snmptrapd	AvEntAmbientTempFlt	8	MAJ	X	ACT	A	YY	
snmptrapd	AvEntAmbientTempOk	8	MAJ	X	RES	A	YY	
snmptrapd	avEntPhyChFruRemoval	9	MAJ	X	ACT	A	YY	
snmptrapd	avEntPhyChFruInsertion	9	MAJ	X	RES	A	YY	
snmptrapd	avEntPhyChFruPsuFlt	10	MAj	X	ACT	A	YY	
snmptrapd	avEntPhyChFruPsuFltOk	10	MAJ	X	RES	A	YY	

GEM alarm rules for the standard traps defined by IETF MIBs

These traps apply to G250/G350/G430/G450 Branch Gateway. All the entries in this file, the syslog entry is should have a unique SNMP trap name. Since there is a unique key in the syslog, the Token2 and Token3 are set to NOT_NEEDED in this file. Token1 in this file will always have the trap name in it.

Note:

The source for all the below rules is STD.

Table 7: Alarm rules

Device	Token 1	evntId	Level	son	type	logId	dest	Description
snmptrapd	coldStart	1	MIN	X	ACT	A	YY	
snmptrapd	warmStart	2	MIN	X	ACT	A	YY	
snmptrapd	linkDown	3	MIN	X	ACT	A	YY	
snmptrapd	linkUp	3	MIN	X	RES	A	YY	

GEM alarm rules for WAN Traps

These traps apply to the G250, G350, and G450 Branch Gateways.

Note:

The source of all the below rules is WAN.

Table 8: Alarm rules

Device	Token 1	evntId	Level	son	type	logId	dest	Description
snmptrapd	wanPhysicalAlarmOn	1	MAJ	X	ACT	A	YY	
snmptrapd	wanPhysicalAlarmOff	1	MAJ	X	RES	A	YY	
snmptrapd	wanLocalAlarmOn	2	MAJ	X	ACT	A	YY	
snmptrapd	wanLocalAlarmOff	2	MAJ	X	RES	A	YY	
snmptrapd	wanRemoteAlarmOn	3	WRN	X	ACT	A	YY	
snmptrapd	wanRemoteAlarmoff	3	WRN	X	RES	A	YY	
snmptrapd	wanMinorAlarmOn	4	WRN	X	ACT	A	YY	
snmptrapd	wanMinorAlarmOff	4	WRN	X	RES	A	YY	
snmptrapd	wanDS1_dup_ip	5	WRN	X	ACT	A	YY	
snmptrapd	wanDS1_ip_vlan	6	WRN	X	ACT	A	YY	
snmptrapd	wanDS1_policyChangeTrap	7	WRN	X	ACT	A	YY	

GEM alarm rules for clock sync and Media Module events

These traps apply to the G250, G350, G430, and G450 Branch Gateways.

Note:

The source of all the below rules is G350.

Table 9: Alarm rules

Device	Token 1	evntId	Level	son	type	logId	dest	Description
snmptrapd	cmgSyncSignalExcess	1	MIN	X	ACT	A	YY	
snmptrapd	cmgSyncExcessClear	1	MIN	X	RES	A	YY	
snmptrapd	lcmgUnsupportedMMEnrollment	3	MAJ	X	ACT	A	YY	
snmptrapd	cmgDataModuleAwohConflict	3	MAJ	X	ACT	A	YY	

GEM alarm rules for Power over Ethernet traps

These traps apply to the G250 and G350 Branch Gateways. All the entries in this file, the syslog entry is has a unique the SNMP trap name. The Token2 and Token3 are, set to NOT_NEEDED in this file.Token1 in this file will always have the trap name in it.

Note:

The source of all the below rules is POE.

Table 10: Alarm rules

Device	Token 1	evntId	Level	son	type	logId	dest	Description
snmptrapd	pethPsePortOnOffNotification	1	WRN	X	ACT	A	YY	
snmptrapd	pethMainPowerUsageOnNotification	2	MIN	X	ACT	A	YY	
snmptrapd	pethMainPowerUsageOffNotification	2	MIN	X	RES	A	YY	

Chapter 7: Other Branch Gateway traps and resolutions

Although alarms can be viewed from the primary server, they are normally resolved from within the Branch Gateway. The Branch Gateway generates the traps listed in the sections below. The sections also provide references to the recommended course of action to resolve the errors indicated by these traps.

Note:

The source of all the below traps is CMG.

cmgMultipleFanClear

Event ID 1

Trap# 3

Alarm Level WRN

Alarm Name cmgMultipleFanClear

Description At least three fans are operating normally. The system should be operable indefinitely without overheating.

cmgPsuFanBriefFault

Event ID 2

Trap# 4

Alarm Level MIN

Alarm Name cmgPsuFanBriefFault

Description 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.

Resolving the problem of a fan operating sub optimally

Procedure

1. Check if there are faults in the system. Use the Branch Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the Branch 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 Branch Gateway for air circulation.
3. If none of the voltages are out of tolerance, but the PSU status indicates failure, replace the entire Branch Gateway. Fans and the PSU are not field replaceable.

cmgPsuFanBriefClear

Event ID 2

Trap# 5

Alarm Level MIN

Alarm Name cmgPsuFanBriefClear

Description The power supply fan is operating normally.

cmgPsuFanProlongedFault

Event ID 3

Trap# 6

Alarm Level MIN

Alarm Name cmgPsuFanProlongedFault

Description 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.

Resolving the problem of a fan operating sub optimally

Procedure

1. Check if there are faults in the system. Use the Branch Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the Branch 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 Branch Gateway for air circulation.
3. If none of the voltages are out of tolerance, but the PSU status indicates failure, replace the entire Branch Gateway. Fans and the PSU are not field replaceable.

cmgPsuFanProlongedClear

Event ID 3

Trap# 7

Alarm Level MIN

Alarm Name cmgPsuFanProlongedClear

Description The power supply fan is operating normally.

cmgCpuTempWarningFault

Event ID 4

Trap# 10

Alarm Level MIN

Alarm Name cmgCpuTempWarningFault

Description The temperature sensor at the CPU has exceeded its warning threshold.

Resolving the rising temperature problem of the CPU

Procedure

1. Check if there are faults in the system. Use the Branch Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the Branch Gateway.
2. If there is a temperature fault, turn off the Branch Gateway and allow it to cool.
3. Reboot the Branch Gateway. Check to see if the fans are working and/or if there is sufficient space around the Branch 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 Branch Gateway.

cmgCpuTempWarningClear

Event ID 4

Trap# 11

Alarm Level MIN

Alarm Name cmgCpuTempWarningClear

Description The temperature sensor at the CPU has dropped below its warning threshold.

cmgDspTempWarningFault

Event ID 5

Trap# 12

Alarm Level MIN

Alarm Name cmgDspTempWarningFault

Description The temperature sensor at the DSP complex has exceeded its warning threshold.

Resolving the rising temperature problem of the DSP complex

Procedure

1. Check if there are faults in the system. Use the Branch Gateway Processor (MGP) Command Line Interface (CLI) command **`show faults`** to display any faults on the Branch Gateway.
2. If there is a temperature fault, turn off the Branch Gateway and allow it to cool.
3. Reboot the Branch Gateway. Check if the fans are working and/or if there is sufficient space around the Branch 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 Branch Gateway.

cmgDspTempWarningClear

Event ID 5

Trap# 13

Alarm Level MIN

Alarm Name cmgDspTempWarningClear

Description The temperature sensor at the DSP complex has dropped below its warning threshold.

cmgMgpPowerFault

Event ID 7

Trap# 16

Alarm Level MAJ

Alarm Name cmgMgpPowerFault

Description The voltage reading at the +5.1V power source serving the Branch Gateway processor is out of tolerance.

Resolving the voltage problem

Procedure

Replace the power supply only if the problem persists. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.

cmgMgpPowerClear

Event ID 7

Trap# 17

Alarm Level MAJ

Alarm Name cmgMgpPowerClear

Description The voltage reading at the +5.1V power source serving the Branch Gateway processor is back within its tolerance range.

cmgMediaModulePowerFault

Event ID 8

Trap# 18

Alarm Level MAJ

Alarm Name cmgMediaModulePowerFault

Description The voltage reading at the -48V power source serving the media modules is out of tolerance.

Resolving the voltage problem

Procedure

Replace the power supply only if the problem persists. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.

cmgMediaModulePowerClear

Event ID 8

Trap# 19

Alarm Level MAJ

Alarm Name cmgMediaModulePowerClear

Description The voltage reading at the -48V power source serving the media modules is back within its tolerance range.

cmgVoipPowerFault

Event ID 9

Trap# 20

Alarm Level MAJ

Alarm Name cmgVoipPowerFault

Description The voltage reading at the +3.4V power source serving the VoIP complexes is out of tolerance.

Resolving the voltage problem

Procedure

Replace the power supply only if the problem persists. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.

cmgVoipPowerClear

Event ID 9

Trap# 21

Alarm Level MAJ

Alarm Name cmgVoipPowerClear

Description The voltage reading at the +3.4V power source serving the VoIP complexes is back within its tolerance range.

cmgDspPowerFault

Event ID 10

Trap# 22

Alarm Level MAJ

Alarm Name cmgDspPowerFault

Description The voltage reading at the +1.58V power source serving the DSP units is out of tolerance.

Resolving the voltage problem

Procedure

Replace the power supply only if the problem persists. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.

cmgDspPowerClear

Event ID 10

Trap# 23

Alarm Level MAJ

Alarm Name cmgDspPowerClear

Description The voltage reading at the +1.58V power source serving the DSP units is back within its tolerance range.

cmg8260PowerFault

Event ID 11

Trap# 24

Alarm Level MAJ

Alarm Name cmg8260PowerFault

Description The voltage reading at the +2.5V power source serving the 8260 processor is out of tolerance.

Resolving the voltage problem

Procedure

Replace the power supply only if the problem persists. Do not replace the power supply if there is a suspected voltage spike or temporary brown-out.

cmg8260PowerClear

Event ID 11

Trap# 25

Alarm Level MAJ

Alarm Name cmg8260PowerClear

Description The voltage reading at the +2.5V power source serving the 8260 processor is back within its tolerance range.

cmgAuxPowerFault

Event ID 12

Trap# 26

Alarm Level MAJ

Alarm Name cmgAuxPowerFault

Description The voltage reading at the -48V auxiliary power source serving the end points is out of tolerance.

cmgAuxPowerClear

Event ID 12

Trap# 27

Alarm Level MAJ

Alarm Name cmgAuxPowerClear

Description The voltage reading at the -48V auxiliary power source serving the end points is back within its tolerance range.

cmgFanPowerFault

Event ID 13

Trap# 28

Alarm Level MAJ

Alarm Name cmgFanPowerFault

Description The voltage reading at the +12V auxiliary power source serving the fans is out of tolerance.

cmgFanPowerClear

Event ID 13

Trap# 29

Alarm Level MAJ

Alarm Name cmgFanPowerClear

Description The voltage reading at the +12V auxiliary power source serving the fans has returned to within its tolerance range.

Branch Gateway cmgSyncSignalFault

Event ID	14
Trap#	30
Alarm Level	MAJ
Alarm Name	cmgSyncSignalFault
Description	Synchronization signal lost.

Restoring the synchronization signal

Procedure

1. Check that the provisioned clock-sync source has a good signal by entering the Branch Gateway Processor (MGP) Command Line Interface (CLI) command **`show sync timing`**.
2. Ensure 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.
3. 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.
4. Enter a **`set sync source`** command to set to the specific MM710 E1/T1 Media Module to be used as the active clock reference.
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 for 2.7 seconds and off for 0.3 seconds, the tone-clock synchronizer is in the **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 for 0.3 seconds and off for 2.7 seconds, the tone-clock synchronizer is in the **active** mode and the internal (on-board) clock is being used as a synchronization reference. Setting the sync timing was not successful.

6. 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 for 2.7 seconds and off for 0.3 seconds, the tone-clock synchronizer is in the **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 for 0.3 seconds and off for 2.7 seconds, the tone-clock synchronizer is in the **active** mode and the internal (on-board) clock is being used as a synchronization reference. Setting the sync timing was not successful.

7. 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.

Branch Gateway cmgSyncSignalClear

Event ID	14
Trap#	31
Alarm Level	MAJ
Alarm Name	cmgSyncSignalClear
Description	Synchronization signal normal.

Branch Gateway cmgVoipHardwareFault

Event ID 15

Trap# 32

Alarm Level MAJ

Alarm Name cmgVoipHardwareFault

Description One or more of the DSP complexes serving the VoIP engines has failed.

Resolving hardware problem related to DSP

Procedure

1. Check the IP configuration.
2. Reset or replace the Media Module.

Branch Gateway cmgVoipHardwareClear

Event ID 15

Trap# 33

Alarm Level MAJ

Alarm Name cmgVoipHardwareClear

Description All of the DSP complexes serving the VoIP engines are back in service.

Branch Gateway cmgModuleRemove

Trap#	50
Alarm Name	cmgModuleRemove
Description	A media modules has been removed.

Branch Gateway cmgModuleInsertFault

Event ID	16
Trap#	52
Alarm Level	MAJ
Alarm Name	cmgModuleInsertFault
Description	Media module insertion sequence has failed.

Resolving a failed media module insertion sequence

Procedure

Reset or replace the media module.

Branch Gateway cmgModuleInsertSuccess

Trap#	53
Alarm Name	cmgModuleInsertSuccess
Description	A media module has been inserted.

cmgMgBusyout

Trap# 54

Alarm Name cmgMgBusyout

Description An administrator has moved a media module or port to the busy-out state.

cmgMgRelease

Trap# 55

Alarm Name cmgMgRelease

Description An administrator has moved a media module or port from the busy-out state back into service.

cmgFirmwareDownloadBegun

Trap# 70

Alarm Name cmgFirmwareDownloadBegun

Description The Branch Gateway has begun download of a software module.

Branch Gateway cmgFirmwareDownloadSuccess

Trap# 71

Alarm Name cmgFirmwareDownloadSuccess

Description The Branch Gateway has completed successful download of a software module.

Branch Gateway cmgRegistrationSuccess

Trap# 73

Alarm Name cmgRegistrationSuccess

Description The Branch Gateway has successfully registered with a controller.

Branch Gateway cmgMgManualReset

Trap# 74

Alarm Name cmgMgManualReset

Description The Branch Gateway is beginning a user-requested reset operation.

Branch Gateway cmgModuleManualReset

Trap# 75

Alarm Name cmgModuleManualReset

Description A media module is beginning a user-requested reset operation.

cmgVoipManualReset

Trap# 76

Alarm Name cmgVoipManualReset

Description A VoIP engine is beginning a user-requested reset operation.

cmgDsuManualReset

Trap# 77

Alarm Name cmgDsuManualReset

Description An E1/T1 DSU is beginning a user-requested reset operation.

cmgConfigUploadBegun

Trap# 78

Alarm Name cmgConfigUploadBegun

Description The Branch Gateway has begun upload of a configuration file.

cmgConfigUploadSuccess

Trap# 79

Alarm Name cmgConfigUploadSuccess

Description The Branch Gateway has completed successful upload of a configuration file.

Branch Gateway cmgMemoryFault

Event ID 17

Trap# 90

Alarm Level MAJ

Alarm Name cmgMemoryFault

Description The Branch Gateway Processor has detected a low processor memory condition.

Resolving a low memory problem

Procedure

1. Check the Branch 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 the 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 is likely that the Branch 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 the trap occurs and does not clear, the Branch Gateway may be functionally impaired. Do not reset the Branch Gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
5. If the trap occurs and the Branch 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.

Branch Gateway cmgMemoryClear

Event ID 17

Trap# 91

Alarm Level MAJ

Alarm Name cmgMemoryClear

Description The main processor memory has returned to normal operation.

Branch Gateway cmgFirmwareDownloadFault

Event ID 19

Trap# 94

Alarm Level MAJ

Alarm Name cmgFirmwareDownloadFault

Description An attempt to download a software module has failed.

Downloading a software module for Branch Gateway

Procedure

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:
   - Exists
   - Has the correct name
   - Resides in the correct directory
3. If the error cannot be resolved after following the above procedure, reboot the Branch Gateway.

cmgProcessRestartFault

Event ID 20

Trap# 96

Alarm Level WRN

Alarm Name cmgProcessRestartFault

Description A software process on the Branch Gateway Processor failed. The Branch Gateway Processor will attempt to restart the failed process. A successful restart of the process will clear this trap.

Restarting a failed software process

Procedure

1. Check the Branch Gateway Processor and ensure 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 the 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 Branch 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 Branch Gateway may be functionally impaired. Reset the Branch 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.

cmgProcessRestartClear

Event ID 20

Trap# 97

Alarm Level WRN

Alarm Name cmgProcessRestartClear

Description Branch Gateway software processes are running normally.

Branch Gateway cmgIccMissingFault

Event ID 21

Trap# 98

Alarm Level MAJ

Alarm Name cmgIccMissingFault

Description An internal communications controller, expected in Slot 1, is missing.

Resolving an issue related to missing internal communications controller

Procedure

1. Check for the presence of an S8300D.
2. If present, check the Branch Gateway administration.
   If the administration is correct, the problem is with the S8300D server.

Branch Gateway cmgIccMissingClear

Event ID 21

Trap# 99

Alarm Level MAJ

Alarm Name cmgIccMissingClear

Description The Internal Communications Controller expected in slot 1 is present.

Branch Gateway cmgIccAutoReset

Event ID 22

Trap# 100

Alarm Level MAJ

Alarm Name cmgIccAutoReset

Description The Branch Gateway automatically reset the Internal Communications Controller.

Resolving the automatic reset problem of the internal communications controller

Procedure

If the problem persists, escalate

Branch Gateway cmgIccAutoResetClear

Event ID 22

Trap# 101

Alarm Level MAJ

Alarm Name cmgIccAutoResetClear

Description The Internal Communications Controller is running normally.

Branch Gateway cmgPrimaryControllerFault

Event ID 23

Trap# 102

Alarm Level WRN

Alarm Name cmgPrimaryControllerFault

Description The Branch Gateway cannot contact the first controller in its controller list.

Contacting the first controller in the controller list

Procedure

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 S8300D Server IP address. If the IP addresses match, go to step 3.
2. If needed, correct this in 'configure' mode on the MGP 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.

Branch Gateway cmgPrimaryControllerClear

Event ID 23

Trap# 103

Alarm Level WRN

Alarm Name cmgPrimaryControllerClear

Description The Branch Gateway successfully contacted the first controller in its controller list.

Branch Gateway cmgNoControllerFault

Event ID 24

Trap# 104

Alarm Level MAJ

Alarm Name cmgNoControllerFault

Description The Branch Gateway cannot contact any controller in its controller list.

Contacting any controller in the controller list

Procedure

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 S8300D. In 'configure' mode on the MGP's CLI, enter **`set mgc list`** with the correct IP address.

Branch Gateway cmgNoControllerClear

Event ID 24

Trap# 105

Alarm Level MAJ

Alarm Name cmgNoControllerClear

Description The Branch Gateway successfully contacted one of the controllers in its controller list.

Branch Gateway cmgRegistrationFault

Event ID 25

Trap# 106

Alarm Level WRN

Alarm Name cmgRegistrationFault

Description The Branch Gateway cannot register with any controllers in its controller list.

Registering with controllers in the controller list

Procedure

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 S8300D 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 S8300D 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 Branch Gateway.

Branch Gateway cmgRegistrationSuccess

Event ID 25

Trap# 73

Alarm Level WRN

Alarm Name cmgRegistrationSuccess

Description The Branch Gateway has successfully registered with a controller.

Branch Gateway cmgH248LinkDown

Event ID 26

Trap# 108

Alarm Level MIN

Alarm Name cmgH248LinkDown

Description The H.248 link between the Branch Gateway and its controller is down.

Fixing the link between the Branch Gateway and its controller

Procedure

1. Check the S8300D Server or duplicated servers.
2. If it is down, bring it up.
3. If it is not, check the Branch Gateway administration.
   Since the following command causes a brief service outage, it should only be executed at the customer convenience.
4. If the administration is correct, reboot the Branch Gateway.
5. If the problem persists, check network connectivity. Use **`ping`** or **`traceroute`** to the S8700-series server or S8300D to check connectivity.
6. If the problem persists, escalate.

Branch Gateway cmgH248LinkUp

Event ID	26
Trap#	109
Alarm Level	MIN
Alarm Name	cmgH248LinkDown
Description	The H.248 link between the Branch Gateway and its controller is down.

cmgTestFault

Event ID	27
Trap#	110
Alarm Level	MIN
Alarm Name	cmgTestFault
Description	Maintenance tests have failed.

Resolving the problem related to failed maintenance tests

Procedure

Refer to the specific maintenance object failure for diagnosis.

cmgTestClear

Event ID	27

Trap# 111

Alarm Level MIN

Alarm Name cmgTestClear

Description Previously failed maintenance tests have passed.

cmgTestThresholdFault

Event ID 28

Trap# 112

Alarm Level MAJ

Alarm Name cmgTestThresholdFault

Description The maintenance test failure count has exceeded its reporting threshold.

cmgTestThresholdClear

Event ID 28

Trap# 113

Alarm Level MAJ

Alarm Name cmgTestThresholdClear

Description The maintenance test failure count has dropped below its reporting threshold.

Branch Gateway cmgMgAutoReset

Event ID 29

Trap# 114

Alarm Level WRN

Alarm Name cmgMgAutoReset

Description The Branch 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 Branch Gateway Processor comes back up after resetting. If the Branch Gateway Processor resets and fails to come back up, this trap will not be generated.

Resolving the automatic reset problem of the Branch Gateway Processor

Procedure

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 Branch Gateway Processor and ensure 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 the trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps.
5. If the trap occurs and the Branch Gateway Processor is frequently resetting, manually reset the Branch Gateway. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.
6. If the trap occurs frequently and the Branch Gateway Processor is not resetting, the Branch Gateway does not function properly and is not capable of resetting itself to restore service. If service is impaired, reset the Branch Gateway manually. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

Branch Gateway cmgModuleAutoReset

Event ID 30

Trap# 116

Alarm Level WRN

Alarm Name cmgModuleAutoReset

Description A Media Module in the Branch Gateway automatically reset (rebooted). A Media Module automatically resets when it fails a sanity test performed by the Branch Gateway Processor.

Resolving the automatic reset problem of a media module

Procedure

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 the trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps.
4. If the trap occurs and the Media Module does not return to service, or if the 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 Branch 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 Branch Gateway Processor

itself. Escalate and have Tier 3 personnel capture the trap information and the event logs for analysis.

Branch Gateway cmgModuleAutoResetClear

Event ID	30
Trap#	117
Alarm Level	WRN
Alarm Name	cmgModuleAutoResetClear
Description	The reset media module is operating normally.

Branch Gateway cmgModulePostFault

Event ID	32
Trap#	118
Alarm Level	MIN
Alarm Name	cmgModulePostFault
Description	A Media Module failed its power-on start-up test.

Resolving a failed power-on start-up test

Procedure

Reset or replace the Media Module.

Branch Gateway cmgModulePostClear

Event ID	32
Trap#	119
Alarm Level	MIN
Alarm Name	cmgModulePostClear
Description	The media module power-on start-up test was successful.

cmgModuleParameterFault

Event ID	33
Trap#	120
Alarm Level	MIN
Alarm Name	cmgModuleParameterFault
Description	A media module failed its parameter exchange.

Resolving a failed parameter exchange of the media module

Procedure

1. Manually reboot the Branch Gateway at a convenient time.
2. If the problem persists, escalate.

cmgModuleParameterClear

Event ID	33
Trap#	121
Alarm Level	MIN
Alarm Name	cmgModuleParameterClear
Description	The media module's parameter exchange succeeded.

cmgConfigUploadFault

Event ID	34
Trap#	122
Alarm Level	MAJ
Alarm Name	cmgConfigUploadFault
Description	An attempt to upload a configuration file failed.

Resolving a failed attempt to upload a configuration file

Procedure

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 Branch Gateway.

Branch Gateway cmgVoipOccFault

Event ID 35

Trap# 124

Alarm Level MIN

Alarm Name cmgVoipOccFault

Description One or more of the VoIP engines in the Branch Gateway is over is its occupancy threshold as measured by a snapshot: (Channels In Use/Total Channels). No action is required.

Branch Gateway cmgVoipOccClear

Event ID 35

Trap# 125

Alarm Level MIN

Alarm Name cmgVoipOccClear

Description All of the VoIP engines in the Branch Gateway are operating below occupancy threshold.

Branch Gateway cmgVoipAvgOccFault

Event ID 36

Trap# 126

Alarm Level MIN

Alarm Name cmgVoipAvgOccFault

Description One or more of the VoIP engines in the Branch Gateway is operating above its average occupancy threshold. No action is required.

Branch Gateway cmgVoipAvgOccClear

Event ID 36

Trap# 127

Alarm Level MIN

Alarm Name cmgVoipAvgOccClear

Description All of the VoIP engines in the Branch Gateway are operating below occupancy threshold.

Branch Gateway cmgVoipAutoReset

Event ID 37

Trap# 128

Alarm Level WRN

Alarm Name cmgVoipAutoReset

Description A VoIP (Voice Over IP) module in the Branch Gateway automatically reset (rebooted). A VoIP module automatically resets when it fails a sanity test performed by the Branch Gateway Processor, when its IP address is administered, or when it fails a ping test performed by the Branch Gateway Processor against the VoIP module's IP address.

Resolving the automatic reset of the VOIP module in the Branch Gateway

Procedure

1. Check if a maintenance test to reset the VoIP module was run.

2. Check if the VoIP module had its IP address re-administered.
3. Check if the IP address administered on the VoIP module is correct.
4. Check if the IP address of the Branch 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 the trap occurs infrequently, the trap may be due to an unusual transient condition. Monitor future traps.
7. If the trap occurs and the VoIP module does not return to service, or if the trap occurs frequently, attempt to reset the failing module from the SAT or CLI and see if this returns it to stable service.
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. Manually reset the Branch 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 Branch Gateway Processor itself. Capture the trap information. If possible, capture the event logs, using the **`show event-log`** CLI command, for analysis. Escalate.
11. If none of this works, capture the trap information. If possible, capture the event logs by using the **`show event-log`** CLI.

Branch Gateway cmgVoipAutoResetClear

Event ID 37

Trap# 129

Alarm Level WRN

Alarm Name cmgVoipAutoResetClear

Description A VoIP engine has completed its automatic reset and is running normally.

cmgDsuAutoReset

Event ID 40

Trap# 132

Alarm Level WRN

Alarm Name cmgDsuAutoReset

Description A DSU in one of the E1/T1 media modules began an automatic reset. No action is required.

cmgDsuAutoClear

Event ID 40

Trap# 133

Alarm Level WRN

Alarm Name cmgDsuAutoClear

Description A DSU in one of the E1/T1 media modules completed its automatic reset and is running normally.

cmgDsuDteDtrFault

Event ID 41

Trap# 134

Alarm Level MIN

Alarm Name cmgDsuDteDtrFault

Description 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.

cmgDsuDteDtrClear

Event ID 41

Trap# 135

Alarm Level MIN

Alarm Name cmgDsuDteDtrClear

Description One of the E1/T1 media modules has detected that the DTR signal from its DTE has returned to normal.

cmgDsuDteRtsFault

Event ID 42

Trap# 136

Alarm Level MIN

Alarm Name cmgDsuDteRtsFault

Description 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.

cmgDsuDteRtsClear

Event ID 42

Trap# 137

Alarm Level MIN

Alarm Name cmgDsuDteRtsClear

Description An E1/T1 media module has detected that the RTS signal from its DTE has returned to normal.

cmgDsuTxDFault

Event ID 42

Trap# 138

Alarm Level MAJ

Alarm Name cmgDsuTxDFault

Description 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.

cmgDsuTxDClear

Event ID 43

Trap# 139

Alarm Level MAJ

Alarm Name cmgDsuTxDClear

Description The E1/T1 media module is receiving normal data from the local DTE to be sent to the far end.

cmgDsuRxDFailure

Event ID 44

Trap# 140

Alarm Level MAJ

Alarm Name cmgDsuRxDFailure

Description 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.

cmgDsuRxDClear

Event ID 44

Trap# 141

Alarm Level MAJ

Alarm Name cmgDsuRxDClear

Description The E1/T1 media module is receiving normal data from the far end to be sent to the local DTE.

Branch Gateway cmgSyncSignalWarn

Event ID 45

Trap# 34

Alarm Level WRN

Alarm Name cmgSyncSignalWarn

Description 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 number 30, cmgSyncSignalFault, is generated.

Branch Gateway cmgSyncWarnClear

Event ID	45
Trap#	35
Alarm Level	WRN
Alarm Name	cmgSyncWarnClear
Description	More than one port is in service on a board that is providing sync timing.

cmgVoipIpConfigFault

Event ID	46
Trap#	142
Alarm Level	MIN
Alarm Name	cmgVoipIpConfigFault
Description	There are two possible causes: a. Duplicate IP address b. VoIP failed to initialize.

Determining the failure

Procedure

Examine the event log to determine the failure that caused the event.

cmgVoipIpConfigClear

Event ID 46

Trap# 143

Alarm Level MIN

Alarm Name cmgVoipIpConfigClear

Description The duplicate IP address has been changed or the VoIP reset to re-initialize.

Trap Number 144

Event ID 47

Alarm Level RES

Description The Branch Gateway is now registered to the reporting server. Alarm has been cleared.

Trap Number 145

Event ID 48

Alarm Level MIN

Description G450/700 Branch Gateway has de-registered (transient loss of registration) from the reporting server.

Trap Number 146

Event ID 49

Alarm Level MAJ

Description G450/700 Branch Gateway has unregistered (registration lost) from the reporting server. All board and call information has been cleared.

Event ID 50

Alarm Level MAJ

Description G350 Branch Gateway is now registered to the reporting server.

Event ID 51

Alarm Level MIN

Description G350 Branch Gateway has de-registered (transient loss of registration) from the reporting server.

Event ID 52

Alarm Level MAJ

Description G350 Branch Gateway has unregistered (registration lost) from the reporting server.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W