Maintenance of the Avaya G350 Media Gateway

555-245-105
Issue 4
January 2005

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

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 may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

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

How to Get Help

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

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. 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.

Standards Compliance

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.

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) – Part 3-3: Limits – Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

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.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. 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.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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 G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

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. 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.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
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-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) 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. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

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

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

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. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

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://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

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 (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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://www.avaya.com/support.

Japan

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。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

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

Contents

About this book

Overview

The *Maintenance of the Avaya G350 Media Gateway* describes the tasks and procedures you perform to maintain the G350 Media Gateway. For instructions on installing and upgrading the components of the Avaya G350 Media Gateway, refer to *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

Audience

The information in this book is intended for use by Avaya technicians, provisioning specialists, business partners, and customers.

Downloading this book and updates from the Web

You can download the latest version of the *Maintenance of the Avaya G350 Media Gateway* from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Web site.

Downloading this book

To download the latest version of this book:

1. Access the Avaya web site at http://www.avaya.com/support.
2. On the left side of the page, click **Product Documentation**.

   The system displays the Welcome to Product Documentation page.
3. On the right side of the page, type **555-245-105**, and then click **Search**.

   The system displays the Product Documentation Search Results page.
4. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book as a zipped PDF file

Related resources

For more information on the Avaya G350 Media Gateway and related features, see the following books:

Title	Number
Overview of the Avaya G350 Media Gateway	555-245-201
Installation and Upgrades for the Avaya G350 Media Gateway	03-300394
Quick Start for Hardware Installation: Avaya G350 Media Gateway	03-300148
Administration of the Avaya G350 Media Gateway	555-245-501
Avaya G350 Media Gateway CLI Reference	555-245-202
Avaya G350 Media Gateway Glossary	555-245-301

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya DEFINITY Helpline at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Trademarks

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.

  Product Documentation Group

  Room B3-H13

  1300 W. 120th Ave.

  Westminster, CO 80234 USA
- E-mail, send your comments to:

  document@avaya.com
- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, *Maintenance of the Avaya G350 Media Gateway*, 555-245-105.

Chapter 1: Maintenance overview

This chapter introduces the Avaya G350 Media Gateway system architecture, and presents an overview of the maintenance strategy for the media gateway and its components.

The G350 with a Media Server system

The G350 with an S8300, S8500, or S8700 Media Server is a family of components that seamlessly delivers a business's voice, fax, and messaging capabilities over an IP network. The value of the G350 system is that it provides a standards-based, IP communications infrastructure that enables Avaya to lower customers' total cost of ownership. The G350 system provides applications to the edge of the network, high reliability for critical applications, and multi-service networking with feature transparency. The G350 with a Media Server infrastructure is comprised of three modular elements: Media Gateways, Media Servers, and Software.

Integration with your network system

The G350 with a Media Server incorporates the following features that help it fit easily into your system:

- It is built around open IP standards (H.248 and H.323).
- It integrates traditional circuit-switched interfaces (analog stations, analog trunks, FAX, multifunction digital stations, T1/E1 trunking, ISDN-BRI and PRI, etc.) and IP-switched interfaces (IP telephones, IP trunking). This integration allows the user to evolve easily from the current circuit-switched telephony infrastructures to next generation IP infrastructures.
- It integrates standard LAN switching capabilities, including Power over Ethernet, and IP routing capabilities with support for WAN technologies like E1/T1 leased lines, PPP, frame relay, USP, and VPN over DSL.

For an overview of the Avaya G350 Media Gateway system, refer to *Overview of the Avaya G350 Media Gateway*, 555-245-201.

For introductory information about the S8300 Media Server or the Avaya G350 Media Gateway hardware, refer to the *Hardware Guide for Avaya Communication Manager*, 555-233-200.

For information on network assessment and readiness testing, refer to *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Maintenance strategy

The maintenance strategy for the Avaya G350 Media Gateway with S8300, S8500, or S8700 Media Servers is intended to provide easy fault isolation procedures and to restrict problems to field replaceable components. The maintenance strategy is driven by the desire to move the G350 towards a data networking paradigm. This leads to a dual strategy in which some of the G350's subsystems are maintained and controlled by a Media Server running Avaya Communication Manager, while others are covered by maintenance software residing on the G350. The latter subsystems are not monitored directly by a Media Server. It is anticipated that future development will enhance the capability of the G350's maintenance software to maintain all subsystems, which will lessen the G350's dependence on a Media Server.

Maintenance of the G350 begins with regular monitoring of the hardware components and software systems of the media gateway. The G350 and its media modules can be monitored in several ways, including:

- Inspecting the G350 and media module LEDs
- Checking the current version of firmware for the G350 and media modules
- Performing facility test calls to test trunks and telephones
- Reviewing the SNMP logs for any traps or alarms

Table 1: Maintenance Interfaces on page 20 shows the main maintenance interfaces associated with the S8300 Media Server and Avaya G350 Media Gateway.

Table 1: Maintenance Interfaces *1 of 2*

Arena	Detail
Web Interface	Web-based access to the S8300/S8500/ S8700 Media Server. Users can perform administration, maintenance, and status functions through the Web interface.
Communication Manager System Access Terminal (SAT) commands	A command line interface, very similar to standard Communication Manager SAT commands that users are familiar with from other Avaya products.

1 of 2

Table 1: Maintenance Interfaces *2 of 2*

Arena	Detail
G350 CLI commands	Unique to the Avaya G350 Media Gateway platform. Used for administration, maintenance, and status functions on the G350.
Avaya G350 Manager	A java-based web management tool for configuring the Media Gateway. Most of the commands available in the CLI are also available through the G350 Manager.
	2 of 2

Media Module maintenance

Procedures for maintenance of Media Modules vary with the type of Media Module being maintained. Data Media Modules, such as the MM314, MM340, and MM342, are administered locally. Voice Media Modules are administered from the server, using Communication Manager. Maintenance for each Media Module is very similar to that for its respective DEFINITY server circuit pack counterpart. Field replacement of Media Modules can be performed in many cases without removing power to the G350 (hot swapping).

Hot swap

The following Avaya Media Modules are hot swappable:

- DCP Media Modules (MM312, MM712, MM717)
- Analog Trunk/Telephone Port Media Module (MM711, MM714)
- T1/E1 Media Module (MM710)
- BRI Media Module (MM720, MM722)

For procedures on adding, removing, or replacing Media Modules, refer to Media Module Replacement on page 41.

CAUTION:

The S8300 Media Server is NOT hot swappable. When removing the S8300, initiate a shutdown process by first depressing the Shut Down button (for 2 seconds) located next to the fourth LED, labelled “Ok-to-Remove” (specific to the S8300). This LED will first blink; then go steady. Once steady, this GREEN LED indicates that the disk drive has been shut down properly and is ready to be removed. If you remove the S8300 before the disk is shut down, you may corrupt important data. See Replacing the S8300 Media Server on page 29.

Note:

The S8300 Media Server can be a primary server for a network of IP endpoints and Avaya G350 Media Gateways, or it can be configured as a Local Survivable Processor (LSP), to become active only if connectivity to the primary server is lost. Most of the material in this book applies to the S8300 Media Server configuration; only a few parts apply to the LSP configuration.

CAUTION:

You can add a data module to the Avaya G350 Media Gateway while the system is running, but the G350 resets when you add the module. However, hot insertion is not recommended in most cases. Because hot insertion resets the G350, any translation and other data that is in the running configuration but has not been saved to the startup configuration will be lost.

LEDs

The general use of LEDs is to give a quick overall understanding of the health of the system and subsystems. When alarms or problems occur, LEDs indicate that attention by a technician is needed. LEDs are not suitable for conveying detailed diagnostic information. Further diagnosis or troubleshooting is supported by software-based solutions that can provide detailed text explaining the error condition. Troubleshooting and diagnostic tasks can be supported by software accessed by laptops in the field or remotely from an administrator’s computer.

The S8300 Media Server and Avaya G350 Media Gateway employ LEDs in the following areas:

- G350 LEDs
- Media Module LEDs (either traditional DEFINITY server or augmented DEFINITY server)
- S8300 LEDs

Detailed descriptions of specific LEDs and their use may be found in Media Module LEDs on page 300.

Maintenance access to the Avaya G350 Media Gateway and Media Servers

You can manage the Avaya G350 Media Gateway using any of the following applications:

- The Avaya G350 Command Line Interface (CLI)
- Avaya G350 Manager
- Avaya Integrated Management
- Avaya QoS Manager

You can access the Avaya G350 Media Gateway and the Avaya S8300 Media Server in several ways:

- Web server access to the Media Gateway or Media Server IP address (accesses Web page with Online Help)
- Telnet from the customer network (LAN or WAN) to:
  - the S8300 IP address
  - the IP address of one of the Avaya G350 Media Gateway interfaces

  Note:

  Since the G350 is also a WAN router, it can have more than one IP interface
- Telnet to the S8300 IP address to port 5023 to get Communication Manager access
- Through Avaya Site Administration
- Remote Telnet/SNMP access via an external serial analog modem connected to the G350 Console port
- Remote Telnet access via an external USB modem connected to the S8300 Media Server
- A console device connected to the CON port on the G350 front panel

  Note:

  For detailed access and login procedures, refer to Chapter 5: Access and login procedures.

Web interface

The browser-based Web administration interface is used to administer the Avaya G350 Media Gateway on the corporate local area network (LAN). This administration interface via the Web is an efficient way to configure the Avaya G350 Media Gateway, the Media Server and Media Modules. In addition to initial administration, it allows you to:

- check server status
- perform software and firmware upgrades
- back up and restore data files

The administration interface via the Web complements the other server administration tools, such as the System Access Terminal (SAT) emulation program and the Avaya Site Administration telephony application. The browser-based Web administration interface focuses on the setup and maintenance of the S8300 Media Server with the Avaya G350 Media Gateway. For more detailed information on access and login procedures, see Connection overview on page 273.

Avaya G350 Media Gateway CLI

The Avaya G350 Media Gateway Command Line Interface (CLI) provides access to configurable and read-only data of all G350 subsystems as well as running tests and displaying results. As a minimum, the CLI supports all functionality the Device Manager provides. It provides access to the status, parameters, and test of Media Modules, IP Entity Configuration, TFTP/FTP Servers, and DSP/VoIP resources. For a detailed description of the CLI commands, refer to the *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

Upgrading software

For information on software upgrades, refer to *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

Plugging in and unplugging the G350

The Avaya G350 Media Gateway contains a detachable power cord. You can power the device by plugging the power cord into the G350 receptacle, then plugging the cord into the wall outlet.

You can remove power by properly powering down the S8300 (see Replacing the S8300 Media Server on page 29), unplugging the power cord from the wall outlet, and then unplugging the power cord from the G350 receptacle.

Note:

The power supply in the G350 is not replaceable.

Note:

Auxiliary power is currently unavailable on the G350.

Useful terms

Table 2: Summary of Terminology on page 25 summarizes some of the terms used in this book, and relates them to former terminology.

Table 2: Summary of Terminology

Present Terminology	Former Terminology
Communication Manager	MultiVantage, Avaya Call Processing
S8300 Media Server	ICC, Internal Call Controller
S8700 Media Server (Could also be a non-co-resident S8300 or S8500)	ECC, External Call Controller

Chapter 2: G350 component maintenance

This chapter describes the maintenance of Avaya G350 Media Gateway components.

G350 component maintenance

Maintenance of the Avaya G350 Media Gateway components is performed by resident software. Components not maintained by the resident software, such as Media Modules, are maintained by Avaya Communication Manager in a manner similar to their DEFINITY server counterparts; see *Maintenance for Avaya DEFINITY® Server R*, 555-233-117.

Power cords

Each G350 Media Gateway ships with one power cord, suitable for the local region. If the power cord provided with the equipment does not have the correct plug configuration needed in a particular country, please refer to the cord set specifications below:

Table 3: Power Cord Specifications

Material Code	Description
174300	US Power Cord
174301	Euro Power Cord
174302	UK Power Cord
174303	Australia Power Cord
174304	India Power Cord
174305	Argentina Power Cord

Following are specifications for power cords suitable for use with the G350:

For North America: The crudest must be UL Listed/CSA Certified, 16 AWG, 3-conductor (3rd wire ground), type SJT. One end is to be terminated to an IEC 60320, sheet C13 type connector rated 10A, 250V. The other end is to be terminated to either a NEMA 5-15P attachment plug for nominal 125V applications or a NEMA 6-15P attachment plug for nominal 250V applications.

For Outside North America: The cord must be VDE Certified or Harmonized (HAR), rated 250V, 3-conductor (3rd wire ground), 1.0 mm minimum conductor size. The cord is to be terminated at one end to a VDE Certified/CE Marked IEC 60320, sheet C13 type connector rated 10A, 250V and the other end to a 3-conductor grounding type attachment plug rated at a minimum of 10A, 250V and a configuration specific for the region/country in which it will be used. The attachment plug must bear the safety agency certifications mark(s) for the region/country of installation.

Replacing the Avaya G350 Media Gateway

Circumstances may require that the Avaya G350 Media Gateway be replaced, either because of hardware or firmware failure, or because of newer technology. Depending upon these circumstances, some or all of the components inserted into the G350 (S8300 Media Server, various Media Modules) may be reused in the replacement G350.

To replace the G350:

1. If the original G350 is still in operation, power down the system. This should be done at a time when there will be the minimum interruption in service.
   a. Perform a shutdown of the S8300 Media Server, if present, using either the Web interface or manually, using the shutdown button on the S8300 faceplate.
   b. Power down the G350 by removing the power cord from the wall power source.
2. Remove all modules from the G350, and carefully set them aside (assuming they will be reused).
3. Reversing the procedures documented in *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394, remove the G350 from its rack mount.
4. Then, following these same procedures, install the replacement G350 hardware into the rack mount.
5. Proceed as you would for the installation of a new G350, following the procedures documented in *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.
6. Install the S8300 Media Server, and any Media Modules according to procedures outlined in *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.
7. Contact RFA, if you have not already done so, and download new license and authentication files to match the serial number of the replacement G350.
8. Following procedures documented in *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394 power up the system, and install the new license and authentication files.
9. In Communication Manager, use the **`change media-gateway`** command to enter the new G350 serial numbers and other data.

Replacing the S8300 Media Server

Circumstances under which it is necessary to replace the S8300 Media Server can include:

- A functional failure on the S8300 board
- A functional failure of the S8300 hard drive
- Replacing an existing S8300 or its hard drive with newer technology

This section describes the following topics:

Backups and restorations

A backup of the system should be performed before the replacement, if possible. Regularly scheduled backups of the system should have been performed as part of ongoing preventative maintenance.

The S8300 system backup should include the following file sets:

- Translation files (not for an LSP)

  Note:
  An LSP receives its translations from the primary server.

- System and server files
- Security files (includes the authentication file but not the license file)

You must generate a new license file for the replacement procedure.

When these files are restored later, it is only necessary to step through the *Configure Server* screens on the Web interface, clicking **Continue**, to read these data into memory.

Manually record the system and server administration information from the *Configure Server* screens during backup, so that this data can be re-entered on the *Configure Server* screens when the translation files and security files are restored later. Table 4: Backup and Restore Requirements on page 30 summarizes these requirements.

Table 4: Backup and Restore Requirements

Communication Manager Version	Backup Files	Restore Files	Configure Server Screens
2.0 or Later	Translations (not for an LSP) System & Server Security	Translations (not for an LSP) System & Server Security	Click Continue, each screen

Server shutdown operations

Depending on the circumstances of the replacement, different server shutdown operations may be required:

1. If you are replacing an active S8300 Media Server, a functional but inactive LSP, or a functional hard drive, you can use the Web interface to shut down the server:
   a. Under **Server**, click **Shutdown This Server**.
   b. On the **Shutdown This Server** screen, the following choices are presented:
      - *Delayed* (default option) – the system waits for processes to close files and other clean-up activities to finish before the server is shut down
      - *Immediate* – the system does not wait for processes to terminate normally before it shuts the server down
   c. Accept the default option.
   d. Leave the check box **After Shutdown, Restart System** unchecked.
   e. Click **Shutdown**.
2. Alternatively, you can manually initiate a shutdown process by first depressing the shutdown button located next to the fourth GREEN “Ok-to-Remove” LED (specific to the S8300) for at least two seconds.
   - For Communication Manager versions 1.2 and earlier, the fourth GREEN “Ok-to-Remove” LED flashes at a constant rate until it finally glows steadily.
   - For Communication Manager version 1.3 and later, the fourth GREEN “Ok-to-Remove” LED flashes at a constant rate, and the TST LED flashes slowly at first. As computer processes exit, the TST LED flashes faster. When the shutdown has completed, the TST LED goes out, and the "OK-to-Remove" LED then glows steadily.

   Once steady, this GREEN “Ok-to-Remove” LED indicates that the disk drive has been parked properly and the S8300 is ready to be removed.

3. If a non-functional S8300, LSP, or hard drive is to be replaced, normal shutdown procedures may not succeed.

   When pressed, the shutdown button programs the S8300 hardware watchdog to reset the module after a two minute fail-safe interval. In addition, recovery measures are taken if the shutdown has not been accomplished within 80 seconds. These recovery measures store diagnostic information in flash memory on the S8300 for later analysis. The LED sequence is different according to the following circumstances:

   a. **Shutdown Failure with Successful Recovery** – If a high priority process has seized control of the S8300's processor, the shutdown signal may be held up indefinitely, so that a shutdown will never proceed. After 80 seconds, a recovery function runs within the S8300's operating system that equalizes process priorities, allowing the shutdown sequence to proceed. The LED sequence is as follows:

      1. After the shutdown button is pressed and held for at least two seconds, the "OK to Remove" LED begins to flash at a constant rate. The TST LED flashes slowly at first.
      2. The TST LED remains flashing at a slow rate for 80 seconds, because shutdown processing is being blocked by runaway processes. After 80 seconds, the YELLOW ACT LED is illuminated, indicating that process priorities have been equalized, and that diagnostic information has been saved for later analysis.
      3. Now allowed to proceed, processes begin to exit as the shutdown begins. As processes exit, the TST LED flashes faster, and the YELLOW ACT LED remains illuminated.
      4. When shutdown has completed, the TST LED goes out, and the "OK to Remove" LED comes on steady. At this point, it is safe to remove the S8300 module from the G350.

   b. **Complete Shutdown Failure** – If an operating system level failure has occurred, it is possible that the processor will never be yielded for the shutdown to begin, even after process priorities are equalized by the recovery function at the 80 second interval. After two minutes, the S8300 will be reset by the hardware watchdog. The LED sequence is as follows:

      1. After the shutdown button is pressed and held for at least two seconds, the "OK to Remove" LED begins to flash at a constant rate. The TST LED flashes slowly at first.
      2. The TST LED remains flashing at a slow rate for 80 seconds, because shutdown processing is being blocked by runaway processes. After 80 seconds, The YELLOW ACT LED is illuminated, indicating that process priorities have been equalized, and that diagnostic information has been saved for later analysis.
      3. Despite the process re-prioritization, the shutdown is still blocked, and the TST LED continues to flash at a slow rate. After two minutes, the hardware watchdog resets the S8300. At this point, the RED ALM LED is illuminated and all others go out. Although this begins restarting the S8300, it will be safe to remove the S8300 module from the G350 for approximately 15 seconds after the module resets.

Removing the S8300 Media Server

The S8300 Media Server contains a Lithium/Manganese Dioxide battery.

CAUTION:

There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Note:

The S8300 Media Server is inserted into the G350 Slot V1, whether it is the primary server or a Local Survivable Processor (LSP). Although the S8300 can fit into any of the slots on the G350, it only functions when inserted in Slot V1 on the left side of the G350. The plate above the slot must be removed to provide clearance for the S8300.

To remove the S8300 Media Server:

CAUTION:

Be sure to wear a properly grounded ESD wrist strap when handling the S8300 circuit board, hard drive, and CWY1. Place all components on a grounded, static-free surface when working on them. When picking up the hard drive, be sure to hold it only on the edges — do not touch the bottom of the hard drive.

1. Shutdown the S8300 Media Server using either the Web interface or the manual shutdown button on the S8300 faceplate (Server shutdown operations).
2. Loosen the two captive screws on the S8300.
3. Remove the plate between slots V1 and V2, labelled “Remove before removing or inserting S8300 module”.
4. Disengage and remove the S8300 from the G350.

Replacing the S8300 Hard Drive

If you are replacing the entire S8300 board, proceed to Reinserting the S8300 Media Server.

To replace the S8300 hard drive, perform the following steps (refer to Figure 1: S8300 Hard Drive Replacement on page 34):

1. Unscrew the four screws on the bottom of the S8300 board that attach to the hard drive standoffs.
2. Remove the hard drive ribbon cable (which is attached to the S8300 board) from the hard drive.

3. If the replacement hard drive does not include them, unscrew the four standoffs from the threaded holes on the bottom of the old hard drive, and screw them into the threaded holes on the bottom of the replacement hard drive.

   CAUTION:

   In Step 4, be careful not to bend the pins on the hard drive. Leave the four jumper pins to the right of the ribbon cable open and unconnected, as shown in Figure 1: S8300 Hard Drive Replacement on page 34.

4. Connect the open end of the hard drive ribbon cable (which is attached to the S8300 board) to the hard drive, as shown in Figure 1: S8300 Hard Drive Replacement on page 34. Connect pin number one to the end of the ribbon connector marked with the red stripe.
5. Place the hard drive on the S8300 board with the standoffs aligned with the screw holes.
6. Hold the S8300 board on its side, with the hard drive in place, and screw the four screws through the bottom of the S8300 board into the hard drive standoffs.

Figure 1: S8300 Hard Drive Replacement

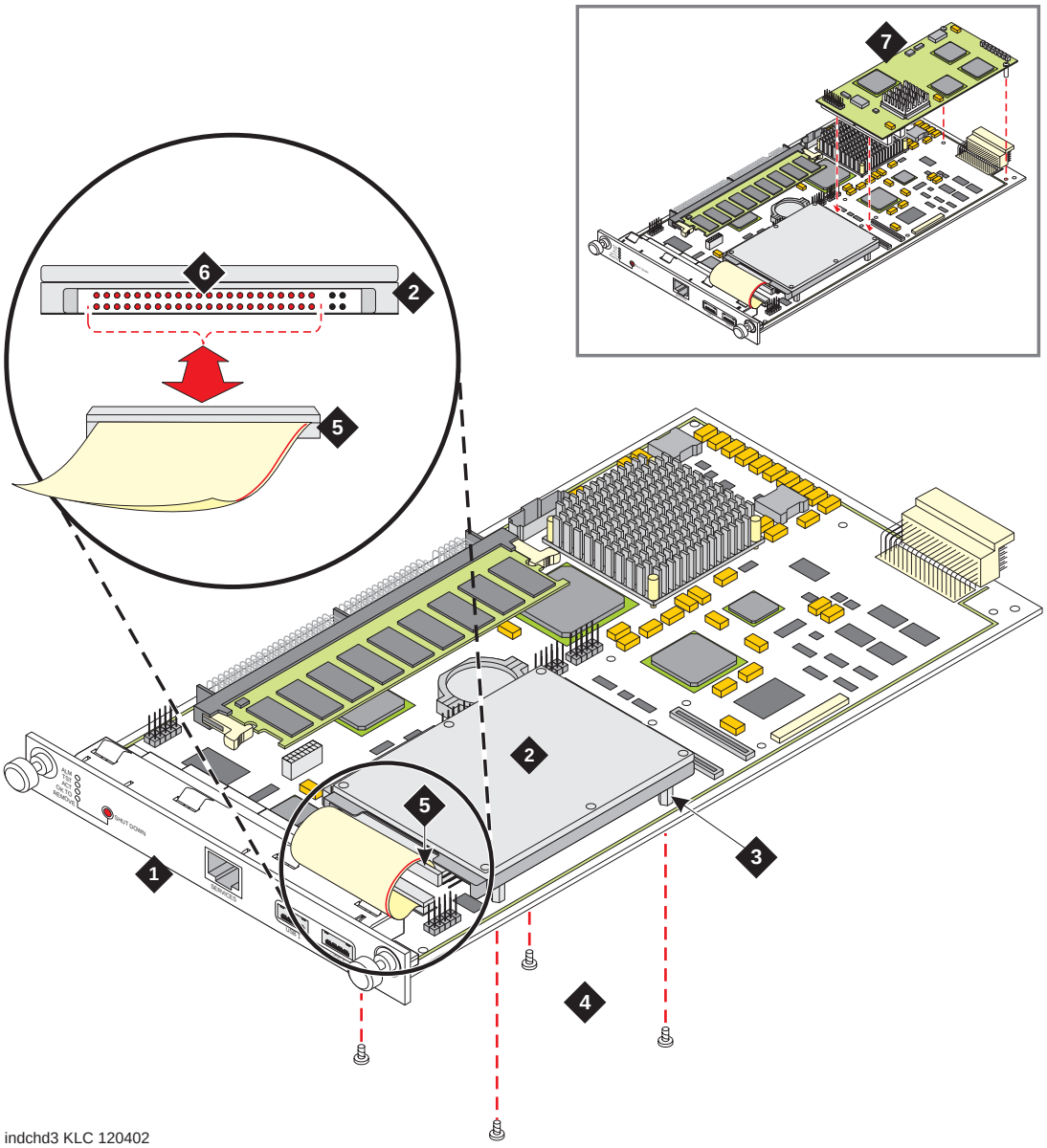


Figure notes:

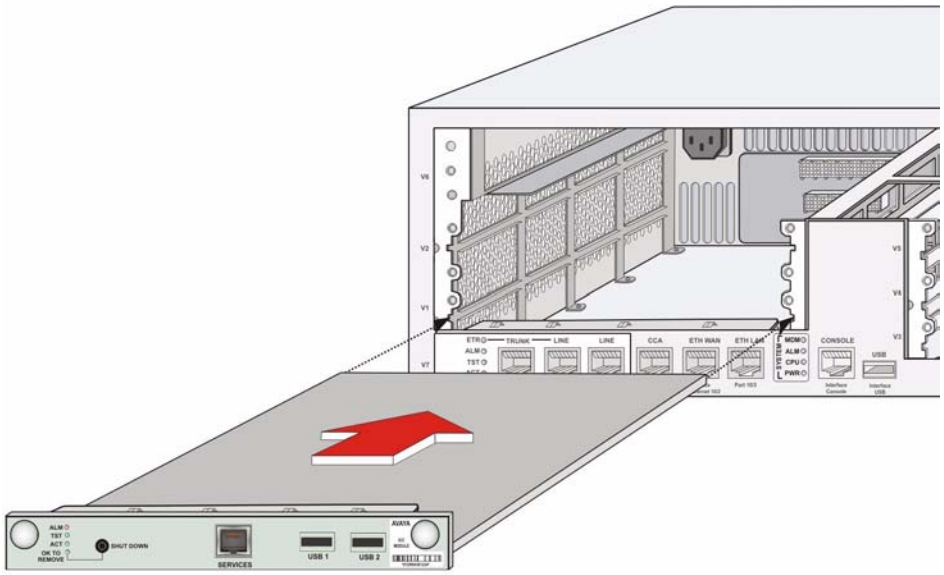
1. **S8300 Circuit Board**
2. **Hard Drive**
3. **Hard-Drive Standoffs**
4. **Screws**
5. **Ribbon Cable Connector**
6. **Hard-Drive Connector Pins**
7. **Optional CWY1 Board**

Reinserting the S8300 Media Server

To reinsert the S8300 Media Server into the G350:

1. Insert the S8300 into slot v1 of the G350 (refer to Figure 2: Align the S8300 Media Server/LSP on page 35).
2. With the optional CWY1 and hard drive attached to the S8300 board, insert the S8300 board about 1/3 of the way into the guides (the guides are in slot v1 for the S8300).
3. Push both boards (together) back into the guides, gently and firmly, until the front of each board aligns with the front of the G350.
4. Secure the S8300 faceplate with the thumb screws. Tighten the thumb screws with a screw driver, in the clockwise direction.
5. Replace the plate between slots V1 and V2, labelled “Remove before removing or inserting S8300 module”.

Figure 2: Align the S8300 Media Server/LSP



WARNING:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Reconfigure the S8300 Media Server/LSP

At the conclusion of the procedure for replacing the S8300 Media Server, the S8300 must be reconfigured for service. Figure 3: S8300 Media Server Replacement Flowchart on page 38 shows several tasks for the G350/S8300 system solution, depending on operational and configuration factors. The letters in the following list correspond to the letters in Figure 3: S8300 Media Server Replacement Flowchart on page 38:

1. Determine whether the replacement S8300 requires an upgrade, or whether the system software requires an upgrade. Using the Web interface, view the version of Avaya Communication Manager on the replacement S8300, and compare it to the version that the system was running before the replacement. Possible outcomes are:
   - Versions identical – No upgrade required (may require patch)
   - Versions different – Upgrade required (may include patch)
2. For the case of no required upgrade, if regularly scheduled backups had been administered for the system:
   a. Install Communication Manager patch, if necessary.
   b. Use the Web interface to restore backup files (according to Table 4: Backup and Restore Requirements on page 30).
   c. Re-install the license file that had been saved on the customer's LAN (or install a new one).
   d. Execute a **`reset system 4`** command to read translations.
   e. Backup system and end procedure.

If no backup exists, proceed with Installation Procedures for a New S8300 Media Server.

3. For the case in which an upgrade is required, two possibilities exist:
   - If the server that was replaced had received regular upgrades and now has a newer version of Communication Manager, the replacement S8300 requires an upgrade. Upgrading the replacement S8300 does not require the installation of a new licence file, because the current license file reflects the newer version of Communication Manager.
   - The replacement S8300 may have been upgraded to a newer version of Communication Manager. In this case, if the upgrade involves a new release of Communication Manager, a new license file must be obtained and installed.
4. If no regularly scheduled backup exists, proceed with Installation Procedures for a New S8300 Media Server. As part of those procedures, performing a necessary upgrade/patch is covered.
5. For the case in which regularly scheduled backups do exist:
   a. Use the Web interface to perform the upgrade.
   b. Install Communication Manager patch, if necessary.

c. Restore backup files (according to Table 4: Backup and Restore Requirements on page 30).

d. Re-install the license file that had been saved on the customer's LAN (or install a new one).

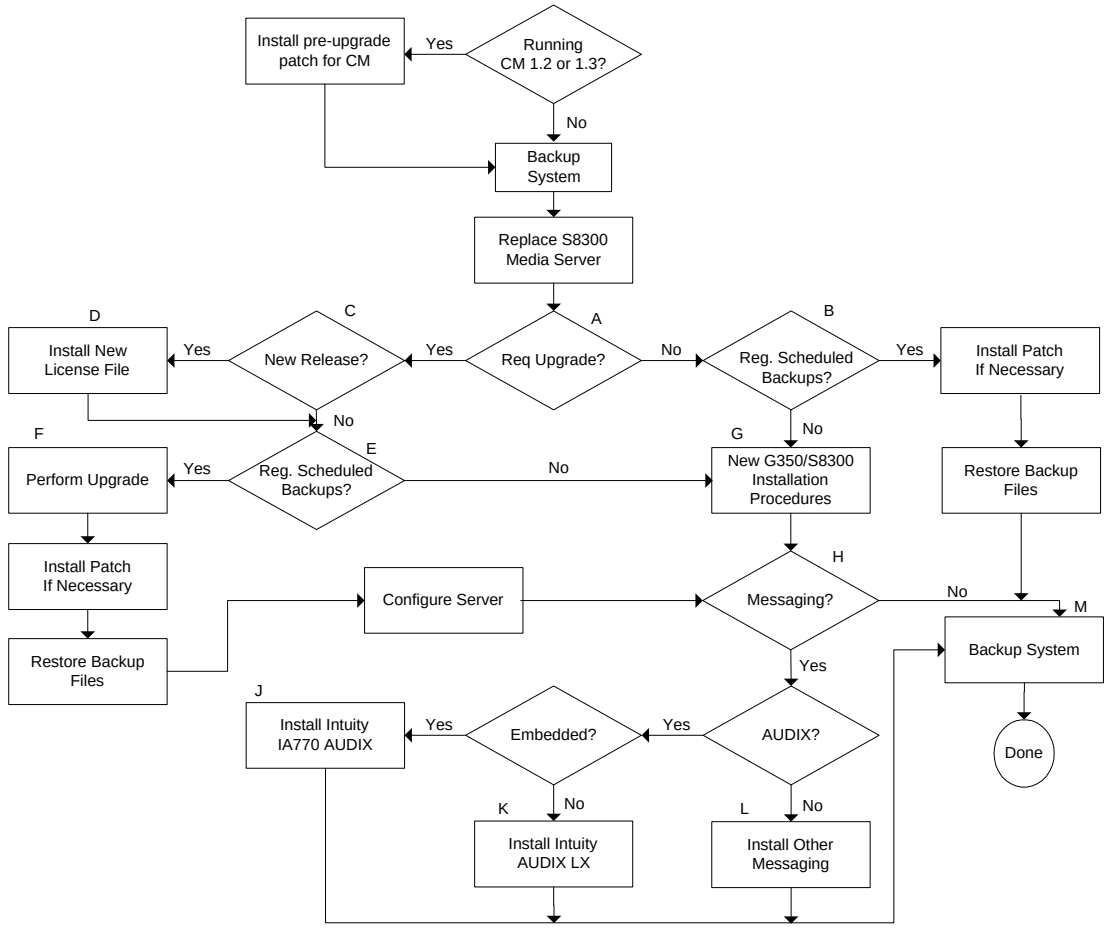
e. Step through the **Configure Server** screens to populate the restored data (as indicated in Table 4: Backup and Restore Requirements on page 30).

Note:

Installation and upgrade procedures for a G350 with an S8300 are described in detail in *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

6. If the configuration has no messaging application, perform another system backup before concluding.
7. If the configuration has a messaging application, install this application. Messaging can be embedded IA770 INTUITY™ AUDIX®, INTUITY™ AUDIX® LX, or another messaging application.
8. For information on installing the IA770 INTUITY AUDIX Messaging Application, refer to *IA770 INTUITY™ AUDIX® Messaging Application*, 555-233-825 on the Avaya S8300 and S8700 Media Server Library CD, or go to http://www.avaya.com/support, select **Communications Systems**, then **Product Documentation**; then, under **Enterprise Class IP Solutions**, select **Avaya G350 Media Gateway and S8300 Media Server**. Finally, search for IA770 INTUITY AUDIX documentation updates.
9. For information on installing the INTUITY AUDIX LX messaging application, refer to *INTUITY™ AUDIX® LX LAN Integration with S8300 and DEFINITY® Systems* on the Avaya S8300 and S8700 Media Server Library CD.
10. If another messaging application is used, follow the installation instructions applicable for that application.
11. Before concluding, perform another system backup.

Figure 3: S8300 Media Server Replacement Flowchart



Media Modules

Supported media modules

The G350 supports the following Avaya media modules:

Table 5: Supported media modules

Media module	Description
S8300	Media server
Telephony media modules	
MM711	8 universal analog ports
MM714	4 analog telephone ports and 4 analog trunk ports
MM312	24 DCP telephone ports
MM712	8 DCP telephone ports
MM717	One amphenol connector that connects to a breakout box or punch down block to provide 24 DCP ports
MM710	1 T1/E1 ISDN PRI trunk port
MM720	8 ISDN BRI trunk ports
MM722	2 ISDN BRI trunk ports
WAN media modules	
MM340	1 E1/T1 WAN port
MM342	1 USP WAN port
LAN media modules	
MM314	24 10/100 Ethernet ports with Power over Ethernet (PoE)

CAUTION:

The MM314 and MM342 are not supported by the Avaya G700 Media Gateway. Do not insert an MM314 or MM342 media module into an Avaya G700 Media Gateway.

The information in Table 6: Equipment List: Media Modules on page 40 is necessary when ordering or replacing Avaya Media Modules.

Note:

ComCode part numbers change frequently. To obtain the most up-to-date ComCode numbers, refer to the Avaya web site.

Table 6: Equipment List: Media Modules

Media Modules		
T1/E1 Media Module		
Material Code: 170900	Apparatus Code: MM710	Optional
DEF DS1 LOOPBACK JACK 700A		
Provides the ability to remotely troubleshoot the T1/E1 Media Module. It is required for any customer with a maintenance contract and highly recommended for any other customer.		
DCP Media Module		
Material Code: 170898	Apparatus Code: MM712	Optional
	BRI Media Module	
Material Code: 170898	Apparatus Code: MM720	Optional
Analog Station/Trunk Media Module		
Material Code: 170899	Apparatus Code: MM711	Optional

Media Module Replacement

Reasons for replacing a Media Module include:

- Repairing a damaged Media Module
- Changing the Media Module type

Since Voice Media Modules on the G350 are administered by Communication Manager, the modules are not inserted until the G350 registers with the Communication Manager. Likewise, all Voice Media Modules and associated Maintenance Objects are removed if the G350 link goes down. Data Media Modules are operational regardless of the G350 registration status.

The term ‘board insertion process’ refers to the process in which the Media Modules are queried as to their type, suffix, and vintage. Use the **`list config all`** or **`list config media-gateway <#>`** commands to access this information. Any Media Module that does not agree with administration generates a process error and is flagged to the relevant administration form.

The removal of Media Modules is detected by the media gateway. Listings of the G350 circuit packs show the relevant slot location as having ‘no board.’ The determination of T1/E1 modes of operation for the DS1 Media Modules is downloadable, since the DS1 Media Module can function as either a T1 or E1 interface.

Upon Media Module replacement, modules are registered with the Avaya G350 Media Gateway, where board type, suffix, and vintage are verified. The G350 then sends appropriate H.248 messages to the controller, creating Communication Manager objects.

You can hot-swap voice modules. This means you can add a voice module to the Avaya G350 Media Gateway while the system is running, without any disruption to your network. Configuration of the G350 is not necessary when you add a voice module. Some configuration of the communication manager is necessary when you install an MM710, MM720, and MM722 Media Module.

You can hot-insert data modules. This means you can add a data module to the Avaya G350 Media Gateway while the system is running, but the G350 resets when you add the module. However, hot insertion is not recommended for data modules in most cases. Because hot insertion resets the G350, any translation and other data that is in the running configuration but has not been saved to the startup configuration will be lost.

Combination Limitations

The following limitations apply to combining media modules in the G350

- Maximum of one MM710 media module
- Maximum of three of the following voice media modules in any combination: MM710, MM711, MM712, MM720, MM714, MM717, or MM722, subject to the following limitations:
  - Maximum of one MM710
  - Maximum of one of the following modules: MM712 and MM717 (you can combine this module with an MM312)

For detailed descriptions of the Media Modules see *Hardware Guide for Avaya Communication Manager*, 555-233-200.

WARNING:

The G350 must not be operated with any slots open. Empty slots should be covered with the supplied blank plates.

CAUTION:

The connector pins can be bent or damaged if the module is handled roughly or if misaligned and then forced into position.

CAUTION:

Separate ESD paths to the chassis ground connect to the Media Modules at the spring-loaded captive screws. Ensure the captive screws are securely tightened to prevent damage to the equipment.

Permitted Slots

The G350 chassis has six media module slots, marked V1, V2, V3, V4, V5, V6. Each media module is restricted to certain slots.

Before inserting Media Modules, consult the following table to find out which Media Modules can be inserted into which slots:

Table 7: Permitted slots for media modules

Media module	Permitted slots
MM312	V6
MM314	V6
MM340	V2, V3, V4, V5
MM342	V2, V3, V4, V5
MM710	V1, V2, V3, V4, V5
MM711	V1, V2, V3, V4, V5
MM712	V1, V2, V3, V4, V5
MM714	V1, V2, V3, V4, V5
MM717	V1, V2, V3, V4, V5
MM720	V1, V2, V3, V4, V5
MM722	V1, V2, V3, V4, V5
S8300	V1

Note:

The MM760 Media Module is currently not supported by the G350.

To replace Media Modules:

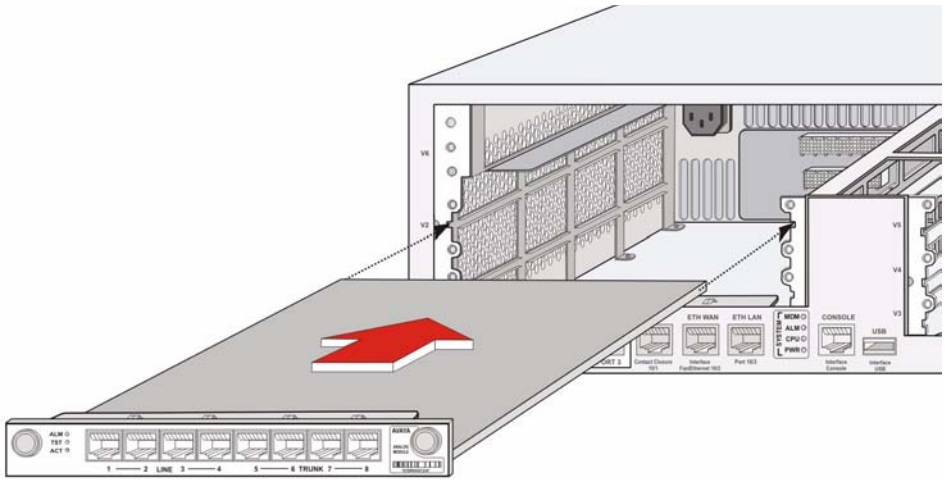
1. Identify and mark all cables.
2. Undo the cables. Make note of the order in which they are removed.
3. Undo the captive screws and slide out the Media Module currently inserted into the G350.
4. Position the Media Module squarely before the selected slot on the front of the G350 chassis and engage both sides of the module in the interior guides.
5. Slide the module slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengage from the guides (Figure 4: Inserting Media Modules on page 43).
6. Apply firm pressure to engage the connectors at the back of the chassis.

   The Media Module connector has different length pins. The long pins engage first to provide grounding. Medium length and short pins provide power and signal.
7. Lock the Media Module into the chassis by tightening the spring-loaded captive screws on the front of the module.
8. Plug in the cables in the correct order (in the reverse of the order in Step 2).

WARNING:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Figure 4: Inserting Media Modules



Facility test call

The facility test call feature allows you to use a voice terminal to make test calls to specific trunks within the system. The test call verifies that the accessed component is functioning properly. To use this feature, it must be enabled on the Class of Restriction form, and you must know the facility test call access code. The code can be retrieved by entering the SAT command **`display feature-access-codes`**. It appears on page one of the screen output.

The trunk test call accesses specific tie or CO trunks, including DS1 trunks. If the trunk is busied out by maintenance, it will be temporarily released for the test call and returned to busyout afterwards. Before making the test call, use **`list configuration`** to determine the location of the trunk ports that you want to test.

Note:

DID trunks cannot be accessed.

Note:

Do not use this trunk test call procedure to test ISDN-PRI or ATM-CES trunks. For more information about testing ISDN-PRI or ATM-CES trunks, see ATM-BCH, Test #258.

To place a test call:

1. Dial the Feature Access Code (FAC) described above and listen for dial tone.
2. If the trunk is on an S8700 PN port, dial the 7-digit port location **UUCSSpp**, where:
   - UU = Cabinet number (01 - 44 for PNs)
   - C = Carrier number (A = 1, B = 2, C = 3, D =4, E = 5)
   - SS = Slot number (01 - 20)
   - pp = Port circuit number (01 - 24)

   The channels on a DS1 trunk are addressed by using the channel number for the port number.
3. If the trunk is on a G350 MM710 Media Module, dial the 7-digit port location **MMMVXyy**, where:
   - MMM = Media Gateway number: 3 digits [0 - 9] [0 - 9] [0 - 9]
   - V = Gateway port identifier carrier = 8
   - On a telephone keypad, the number “8” also displays the letters “T”, “U”, and “V”.
   - X = Slot number (1 - 5, if no S8300/LSP in Slot 1)
   - yy = Circuit number

Circuit range depends upon the Media Module on which the trunk is set up. For the Avaya Analog Media Module (MM711), the range is 1-8; for the Avaya T1/E1 Media Module (MM710), the range could be 1-23, 1-24, 1-31, or 1-32, depending upon the type of translation and signaling.

Example: If the CO trunk is on port 5, MM in slot 3, of MG 34,

dial FAC

get dial tone

dial 0348305

4. Listen for one of the following tones:

Tone	Description / Steps
Dial tone or silence	The trunk is connected. Go to Step 5.
Busy tone	The trunk is either busy processing a call or is out of service. Check **status trunk**.
Reorder tone	The trunk requested is in a different port network from your station, and inter-PN resources are not available to access it.
Intercept tone	The port addressed is not a trunk, or it is a DID trunk, or the trunk is not administered.
Confirmation tone	The port is a tone receiver.

5. Place a call. If the call does not go through (no ringing is heard), check to see if the circuit has been removed or if the trunk is a rotary trunk.

   The dial tone heard is coming from the far-end. If the far-end has been disabled, you will not hear dial tone. However, depending on far-end administration, you may still be able to dial digits. Every digit dialed after the port number is transmitted using end-to-end DTMF signaling. If the trunk being tested is a rotary trunk, it is not possible to break dial tone.

Setting G350 synchronization

If the Avaya G350 Media Gateway contains an MM710 T1/E1 Media Module, it is usually advisable to set the MM710 up as the primary synchronization source for the G350. In so doing, clock sync signals from the Central Office (CO) are used by the MM710 to synchronize all operations of the G350. If no MM710 is present, it is not necessary to set synchronization.

If Communication Manager is running on an Avaya S8300 Media Server, however, the usual SAT screens for “display sync” and “change sync” are not present. Clock synchronization is set via the Media Gateway command line interface (CLI). The command **`set sync interface {primary | secondary} {<mmID> | [<portID>]}`** defines a potential stratum clock source (T1/E1 Media Module, ISDN-BRI), where:

- *<mmID>* is the Media Module ID of an MM stratum clock source of the form “vn”, where “n is the MM slot number, and
- *<portID>* (for the MM720 BRI Media Module) is formed by combining the mmID of the MM to the 2-digit port number of the BRI port.

Note:

If the **`add ds1`** command has not been run in the Communication Manager, the **`set sync interface`** command will not work.

By setting the clock source to **`primary`**, normal failover will occur. Setting the source to **`secondary`** overrides normal failover, generates a trap, and asserts a fault. The identity of the current sync source in use is not stored in persistent storage. Persistent storage is used to preserve the parameters set by this command.

Control of which reference source is the “Active” source is accomplished by issuing the command **`set sync interface {primary | secondary}`**. If **`secondary`** is chosen, then the secondary source becomes “Active”, and the primary becomes “standby”. In addition, fallback to the primary source will not occur if or when it becomes available.

If neither primary nor secondary sources are identified, then the local clock becomes “Active”.

To set the MM710 as the primary synchronization source:

1. Login at the **Welcome to Media Gateway Server** menu.
   You are now logged-in at the Supervisor level on the Media Gateway. The prompt appears as **G350-mmm(super)#**, where **mmm** is the administered G350 Media Gateway number in the network.
2. At the prompt, type **`set sync interface primary <mmid>`**.
   The MM710 Media Module is now configured as the primary clock synchronization source for the Avaya G350 Media Gateway.
3. At the prompt, type **`set sync source primary`**.

If the Avaya G350 Media Gateway contains a second MM710 Media Module, type **`set sync interface secondary`**. If, for any reason, the primary MM710 Media Module cannot function as the clock synchronization source, the system defaults to the secondary MM710 Media Module for that function. If neither MM710 Media Module can function as clock synchronization source, the system defaults to the local clock running on the S8300 Media Server.

The YELLOW ACT LED on the front of the MM710 Media Module can tell you the synchronization status of that module.

- If the YELLOW ACT LED is solidly on or off, it has NOT been defined as a synchronization source. If it is on, one or more channels is active. If it is an ISDN facility, the D-channel will count as an active channel and will cause the YELLOW ACT LED to be on.
- When the MM710 is driving a clock sync source line to the G350 main clock, the YELLOW ACT LED does not indicate port activity, but instead indicates that the MM710 is the sync source by flashing with a regular 3-second period:
  - It is on for 2.8 seconds and flashes off for 200 milliseconds if it has been specified as a sync source and is receiving a signal that meets minimum requirements for the interface.
  - If it has been specified as a sync source and is not receiving a signal, or is receiving a signal that does not meet minimum requirements for the interface, then the YELLOW ACT LED will be off for 2.8 seconds and flash on for 200 milliseconds.

Viewing G350 sync sources

The following tables illustrate example configurations of the clock synchronization sources:

Note:

Unless otherwise indicated, the following commands are sent from the G350 Media Gateway CLI.

Table 8: G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary		Not Configured	
Secondary		Not Configured	
Local	V0	Active	None
Comment: No failures, SIG GREEN on and ACT on when trunk is seized			

Table 9: G350-001# set sync interface primary v4
G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Locked Out	None
Secondary		Not Configured	
Local	V0	Active	None
Comment: No failures, Sig is green and ACT On 2.8s off 0.2s Note that the MM710 in slot 4 has been declared to be the primary sync source but it is not active until the next command is sent.			

Table 10: G350-001# set sync source primary
G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Active	None
Secondary		Not Configured	
Local	V0	Standby	None
Comment: The ACT LED does not change its behavior.			

Note:

The following command is sent from the SAT CLI, and *not* from the G350 CLI.

To test for slippage, from the SAT, use the command:

```
test mo logical 4255 physical 1v4 test 144
```

The results from the above command are shown in Table 11: TEST RESULTS on page 48:

Table 11: TEST RESULTS

Port	Maintenance Name	Alt. Name	Test No. Result	Error Code
001V4	MG-DS1	144	PASS	
Command successfully completed				

If a secondary sync source is similarly provisioned:

Table 12: G350-001# set sync interface secondary v3 G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Active	None
Secondary	V3	Standby	None
Local	V0	Standby	None

To activate the secondary sync source:

Table 13: G350-001# set sync source secondary G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Locked Out	None
Secondary	V3	Active	None
Local	V0	Standby	None
Note: The system uses one clock at a time only: therefore only the secondary is active and the primary is locked out.			

To activate the local sync source:

Table 14: G350-001# set sync source local G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Locked Out	None
Secondary	V3	Locked Out	None
Local	V0	Active	None

To reactivate the primary sync source:

Table 15: G350-001# set sync source primary
G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Active	None
Secondary	V3	Standby	None
Local	V0	Standby	None
Note that secondary and local are standby because they are provisioned as fail overs.			

If the T1 physical connection is removed, then the secondary becomes active and the primary reports a failure.

Table 16: G350-001# show sync timing

SOURCE	MM	STATUS	FAILURE
Primary	V4	Standby	Out of Lock
Secondary	V3	Active	None
Local	V0	Standby	None
Note that primary and local are standby because they are provisioned as fail overs.			

IP telephones

Note:

Refer to *4600 Series IP Telephone LAN Administration*, 555-233-507 for troubleshooting details and error codes, as well as the phone administration information.

The Avaya 4600-Series IP Telephones are relatively trouble-free. Table 17: IP Phone Problems and Solutions on page 51 provides the most common problems an end user might encounter. For other IP Telephone questions or problems, contact your Telephone System Administrator. Some typical problems are:

- Phone does not activate after connecting it the first time
- Phone does not register after a power interruption
- Characters do not appear on the display screen
- Display shows an error/informational message
- No dial tone
- Echo, noise or static when using a headset
- Phone does not ring
- Speakerphone does not operate
- A feature does not work as indicated in the User Guide

Table 17: IP Phone Problems and Solutions *1 of 3*

Problem/Symptom	Suggested Solution
Phone does not activate after connecting it the first time	Unless your System Administrator has already initialized your telephone, you may experience a delay of several minutes before it becomes operational. Upon plug-in, your telephone immediately begins downloading its operational software, its IP address and any special features programmed by your System Administrator from the server to which it is connected. Report any delay of more than 8-10 minutes to your System Administrator.
Phone does not activate after a power interruption	Allow a few minutes for re-initialization after unplugging, powering down the phone, server problems or other power interruption.

1 of 3

Table 17: IP Phone Problems and Solutions *2 of 3*

Problem/Symptom	Suggested Solution
Characters do not appear on the Display screen	See *Phone does not activate after connecting it the first time* above. Check the power source to be sure your telephone is receiving power. Check all lines into the phone to be sure it is properly connected. Perform the Test procedure: with the telephone idle, press and hold the **Trnsfr** button; the line/feature indicators should light and the display should show all shaded blocks. Release the **Trnsfr** button to end the test. If the above suggested solutions do not resolve the problem, reset or power cycle the phone.
Display shows an error/ informational message	Most messages involve server/phone interaction. If you cannot resolve the problem based on the message received, contact your Telephone System Administrator for resolution.
No dial tone	Make sure both the handset and line cords into the phone are securely connected. Note that there may be a slight operational delay if you unplug and reconnect the phone. If you have a 4612 or 4624 IP Telephone, check to be sure the phone is powered (press **Menu**, then **Exit**); if nothing appears on the display, check your power source. If you have a 4612 or 4624 IP Telephone, check to be sure your phone is communicating with the switch; press **Menu**, then any of the softkey features (e.g., Timer). If the selected feature activates, the switch/ IP phone connection is working. Reset or power cycle the phone. See your Telephone System Administrator if the above steps do not produce the desired result. Check the status of the VoIP board.

2 of 3

Table 17: IP Phone Problems and Solutions *3 of 3*

Problem/Symptom	Suggested Solution
Echo, noise or static when using a headset; handset operation works properly	Check the headset connection. If the connection is secure, verify that you are using an approved headset, base unit and/or adapter, as described in the list of approved Avaya Communication compatible Headsets.
Phone does not ring	If you have a 4612 or 4624 IP Telephone, use the Menu to access the **RngOf** (Ringer Off) feature; if a carat (downward triangle) appears above that feature, your phone is set to not ring. To correct, press the softkey below **RngOf**; when the carat does not display, your ringer is active. If "Ringer Off" is programmed on a Line/ Feature button, that button's indicator light will appear as steady green; reactivate the ringer by pressing that Line/Feature button again. Set your ringer volume to a higher level using the Up/Down Volume keys. From another phone, place a call to your extension to test the above suggested solutions.
Speakerphone does not operate	Ask your System Administrator if your speakerphone has been disabled.
A feature does not work as indicated in the User Guide	Verify the procedure and retry. For certain features, you must lift the handset first or place the phone off-hook. See your Telephone System Administrator if the above action does not produce the desired result; your telephone system may have been specially programmed for certain features applicable only to your installation.
All other IP Phone problems	Contact your Telephone System Administrator.

3 of 3

Reset and power cycle

Reset your IP Telephone when other Troubleshooting suggestions do not correct the problem. Use a Power Cycle with the approval of your System Administrator only when a reset does not resolve the problem.

Reset your phone

This basic reset procedure should resolve most problems.

To reset your phone:

1. Press **Hold**.
2. Using the dial pad, press the following keys in sequence: **73738#**

   The display shows the message “Reset values? * = no # = yes.”
3. Choose one of the following from Table 18: Resetting the Phone on page 54:

Table 18: Resetting the Phone

If you want to	Then
Reset the phone without resetting any assigned values	Press * (asterisk). A confirmation tone sounds and the display prompts "Restart phone? * = no # = yes."
Reset the phone and any previously assigned (programmed) values (Use this option only if your phone has programmed, static values)	Press # (the pound key) The display shows the message “Resetting values” while your IP Telephone resets its programmed values, such as the IP address, to its default values, and re-establishes the connection to the server. The display then prompts “Restart phone? * = no # = yes.”

4. Press # to restart the phone or * to terminate the restart and restore the phone to its previous state.

Note:

Any reset/restart of your phone may take a few minutes.

Power cycle the phone

Use the power cycle only if the basic or programmed reset procedure cannot be performed or does not correct the problem.

To power cycle the phone

1. Unplug the phone and plug it back in.
   The phone connection is re-established.

If power-cycling does not correct the problem, a more severe power cycle routine can be performed by unplugging both the phone and the Ethernet cables. However, because this type of power cycle involves reprogramming certain values, it should only be performed by your Telephone System Administrator.

Chapter 3: Avaya Communication Manager controlled maintenance

This chapter addresses Avaya G350 Media Gateway subsystems and components that are controlled by Avaya Communication Manager SAT commands.

G350 subsystems maintained by Communication Manager

Communication Manager subsystems can be listed via the **`list config`** command and, in most cases, have some maintenance activities involved.

Note:

`list config all` on the Communication Manager SAT gives you complete information, including whether or not stations have been administered on a port. **`show mg list_config`** on the G350 CLI gives you information for the installed equipment in that G350.

The G350 subsystems that are applicable to Communication Manager maintenance considerations are identifiable by the presence of ‘angels’. Angels may be either physical or virtual, and both types use the CCMS message.

Maintenance commands

DEFINITY server-experienced users will find that G350 components and Media Modules function, and are maintained, in a similar way as their DEFINITY server counterparts.

Categories of maintenance commands

- Communication Manager SAT commands
- Avaya G350 Media Gateway CLI commands

Since the Media Modules have many of the same Maintenance Objects as the DEFINITY server circuit packs, many of the same operations apply, as follows:

- The **`test mo logical xxx physical xxx`** command works with the physical address of a Media Module Maintenance Object.
- The **`enable/disable MO logical xxx physical xxx`** commands work with the physical address of a Media Module Maintenance Object.
- All Voice Media Modules and their associated ports can be busied out and released from the busyout state on demand from the SAT.

  Note:

  A Communication Manager warning alarm and associated hardware error with error code 18 is generated when a Media Module is busied out.

- All Media Modules can be reset on demand from the SAT by use of the **`reset board`** command.

  CAUTION:

  This is a destructive command so the Media Module must be busied out before a demand reset can be done.

- If an invalid G350 number is entered with the test command for a Media Module board or port, the following message is displayed: **"xxxx" port/board is not valid**.
- Tests that are called for but that cannot run on a Media Module abort with the abort code 1412.
- A request for a demand test, a reset, or busy out of the module (board) location for the S8300 Media Server aborts.

SAT commands specific to the Avaya G350 and G700 Media Gateways

In traditional servers running Communication Manager, ports are identified by the cabinet number, carrier, slot, and port (e.g., 01A0704). This naming convention does not make physical sense for Media Modules. Therefore, a new convention was developed that meets the needs of the Avaya G350 and G700 Media Gateways, yet for portability to traditional administration maintains the 7 character field. Also, in traditional server administration there are many commands that either require port fields as an argument to the command or require a port field value be entered on the form. Therefore these commands need to understand Media Module port fields and accept them as valid entries. This applies to both the S8300 Media Server and an external communications controller, whether it be an S8700 Media Server or another server. The media gateway format is GGGVMPP, where GGG is the media-gateway number, VM is the module slot number, and PP is the port number.

Note:

The V, for virtual, is a required character that is part of the module slot number (H.248 terminology).

The following subsections describe the commands unique to the Avaya G350 and G700 Media Gateways:

- add/change/display/status media gateway [x, next]
- list media-gateway
- list configuration media-gateway
- status media-gateway

add/change/display/status media gateway [x, next]

Figure 5: Media-Gateway Administration Screen

The Avaya G350 and G700 Media Gateways Primary Server administers the Avaya G350 and G700 Media Gateways by the command **`add media-gateway x`** or **`add media-gateway next`**, where *x* is valid between the range of 1 to the capacity for a given primary server, and *next* is the next available number to be administered.

The commands **`change media-gateway x`**, **`display media-gateway x`**, and **`remove media-gateway x`** are supported in the same manner as the **`add media-gateway x`** command.

Media Gateway form fields

The Media Gateway form contains the following editable fields:

- **Number** – the number of the media gateway (1 – 50)
- **Type** – the type of media gateway (g350 or g700)
- **Name** – a 20-character text string containing a meaningful identifier for the media gateway

- **Serial No.** – the serial number of the media gateway
- **Network Region** – a two or three character field specifying which IP network region the media gateway resides in. The network region is used by the primary server to allocate resources from the nearest Media Gateway.

  The number of characters is dependent upon the type of primary server. The default is a blank field.
- **Encrypt Link?** – indicates whether the H.248 signaling link should be encrypted
- **Location** – the location number of the media gateway's location

  The default is one (1).
- **Site Data** – a text string containing a meaningful identifier for the site
- **V1** – the only slot that can contain an S8300. It can also contain other Media Modules if there is no S8300 in the system.
- **V2 - V5** – general slots for G350/G700 form factor Media Modules
- **V6** – the only slot that can contain the MM312 and MM314 Media Modules
- **V7** – the virtual slot from which the analog ports on the motherboard are administered
- **V9** – the virtual slot from which the integrated announcements are administered

The Media Gateway form has several additional fields for display purposes only:

- **Registered?** – the 'Registered?' field is one (1) character long for indicating whether an Avaya G350 Media Gateway or G700 Media Gateway is currently registered with the primary server or not. The 'Registered?' field is a display only field. The 'Registered?' field can have a value of y(es) or n(o).
- **IP Address** - the IP Address field is a 15 character display only field containing the IP Address of the media gateway. The data in this field is of the form: XXX.XXX.XXX.XXX (where XXX is a decimal value between 000 and 255). The IP address field returns a blank field until the Media Gateway registers for the first time. Once the G350/G700 registers, that IP address is always displayed, even if the G350/G700 becomes unregistered, until a G350/G700 with a different IP address is validly registered with the same administered identifier. The populated IP address is persistent over reboots.
- **FW Version** – displays status information on the change media gateway command
- **MAC Address** - the MAC Address field is a 17 character display only field containing the MAC Address of the media gateway. The data in this field is of the form: XX:XX:XX:XX:XX:XX (where XX is a hexadecimal value between 00 and FF). The MAC Address field returns a blank field until the G350/G700 registers for the first time. Once the G350/G700 registers, that MAC Address is always displayed, even if the G350/G700 becomes unregistered, until a G350/G700 with a different MAC Address is validly registered with the same administered identifier.
- **Controller IP Address** – displays status information on the change media gateway command

The Avaya G350 Media Gateway Media Modules are listed by Slot V1-V6, followed by the input field for ‘Module Type’. The Avaya Media Modules can be one of six types: analog, **BRI**, DCP, ETH 24P, ICC, or DS1 (also referred to as T1/E1). The default for the Module Type field is a blank field.

Note:

The S8300 Media Server and LSP are both processor-type Media Modules. From a SAT administration view-point, there is no difference between the S8300 Media Server and LSP; therefore, the designation for both is via icc in the Module Type field.

If an administered Media Module is in conflict with the inserted Media Module, then a pound sign (#) is displayed to the left of the ‘Module Type’ field on the Media Gateway form and the following footnote is displayed: “**‘#’ indicates module type conflict**”.

list media-gateway

From the **primary server**, the **`list media-gateway`** command shows all Avaya G350 and G700 Media Gateways currently administered.

Note:

The “print” modifier is supported on Linux and Windows platforms only if the terminal type for the command is 4410. Any other terminal type returns the error message: “**pr not supported by platform**”.
Printer support may be provided by administering a switch-to-printer TCP/IP connection on the customer’s LAN. To do this, administer the following:

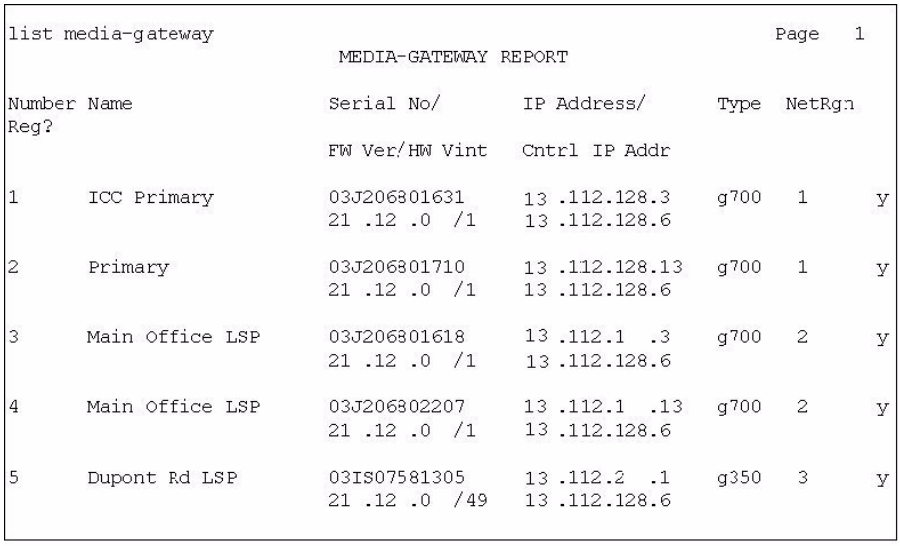
- Node names and IP addresses for the switch and the terminal server on the **node names ip** form
- Service types, local nodes, and remote nodes on the **ip services** form
- TCP “listen” port on the terminal server

For more information on procedural details, refer to *Administering a TCP/IP printer connection* under *Printer translations (switch)* in *Translations and testing* of the *GuestWorks® and DEFINITY® Systems Technician Handbook for Hospitality Installations*, 555-231-743.

The **`list media-gateway`** command displays the current status for the media gateways using the following fields:

- **Registered?** – indicates whether the media gateway is currently registered
- **IP Address** – indicates the IP address of the media gateway
- **FW Version/HW Version** – shows the firmware version number and the hardware version number for the media gateway
- **MAC Address** – shows the MAC address of the media gateway
- **Controller IP Address** – indicates the IP address of the controller with which the media gateway is currently registered.

Figure 6: List Media-Gateway Screen



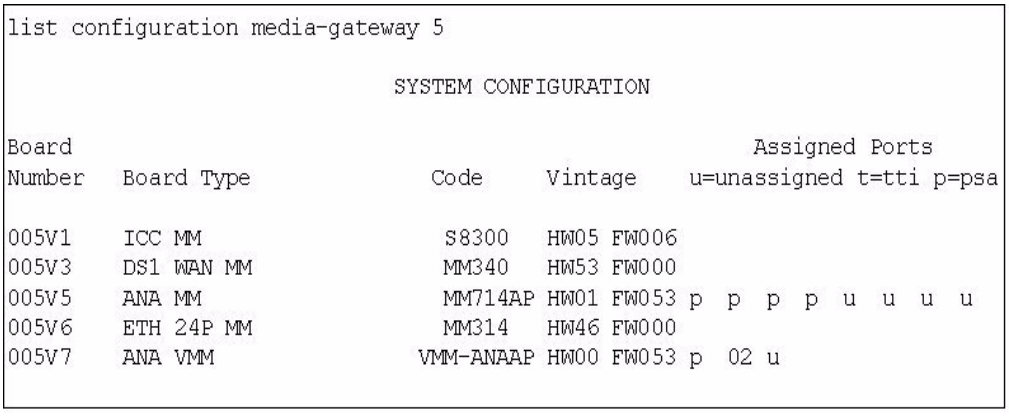
```
list media-gateway                                              Page   1
                          MEDIA-GATEWAY REPORT

Number Name                Serial No/       IP Address/      Type  NetRgn
Reg?
                           FW Ver/HW Vint   Cntrl IP Addr

1      ICC Primary         03J206801631     13 .112.128.3    g700   1      y
                           21 .12 .0  /1    13 .112.128.6

2      Primary             03J206801710     13 .112.128.13   g700   1      y
                           21 .12 .0  /1    13 .112.128.6

3      Main Office LSP     03J206801618     13 .112.1  .3    g700   2      y
                           21 .12 .0  /1    13 .112.128.6

4      Main Office LSP     03J206802207     13 .112.1  .13   g700   2      y
                           21 .12 .0  /1    13 .112.128.6

5      Dupont Rd LSP       03IS07581305     13 .112.2  .1    g350   3      y
                           21 .12 .0  /49   13 .112.128.6
```

The IP address field returns a blank field until a media gateway registers for the first time. Once the media gateway has registered, that IP address is always displayed, even if the media gateway becomes unregistered, until a media gateway with a different IP address is validly registered with the same administered identifier. The populated IP address is persistent over reboots.

list configuration media-gateway

The command **`list configuration media-gateway`** ***x*** lists all the assigned ports on the Media Modules for the specified Media Gateway.

Figure 7: List Configuration Media-Gateway Screen



```
list configuration media-gateway 5

                              SYSTEM CONFIGURATION

Board                                                      Assigned Ports
Number   Board Type              Code     Vintage    u=unassigned t=tti p=psa

005V1    ICC MM                   S8300   HW05 FW006
005V3    DS1 WAN MM               MM340   HW53 FW000
005V5    ANA MM                   MM714AP HW01 FW053 p  p  p  p  u  u  u  u
005V6    ETH 24P MM               MM314   HW46 FW000
005V7    ANA VMM                VMM-ANAAP HW00 FW053 p  02 u
```

The output from the **list configuration media-gateway *x*** command displays a fixed number of assigned ports for the following Media Module types: analog(8), DCP(8), BRI(8), DS1(32), MM314 ETH 24P (None), MM312 DCP (24), MM722 BRI (4), MM720 BRI (16), and ICC (None).

Note:

Those with “None” as the number of assigned ports display blanks.

Each of the assigned Media Gateway ports are labeled as ‘u’ for unassigned, ‘t’ for TTI, ‘p’ for PSA or a value between 01 and the max number of assigned ports for each Media Module type when that port is assigned.

Module Number displays in the format of GGGVM, where GGG is the media gateway number and VM is the module number.

Module Types display as *‘ANA MM’, ‘ANN MM’, ‘BRI MM’, ‘DCP MM’, ‘DS1 WAN MM’, ‘ICC MM’, ‘ANA VMM’.*

Module Vintage is displayed for both the hardware and firmware.

status media-gateway

The **status media-gateway** command displays the alarm status for the administered media gateways. This command lists alarms, lists busied out trunks and stations, and lists how many H.248 links are up and down for all media gateways. The alarms displayed here are only associated with board type alarms on the Media Modules. Status for VoIP and Media Gateway alarms are provided via the Media Gateway Processor CLI.

Figure 8: Status Media-Gateways Screen

```
status media-gateways


  ALARM SUMMARY    BUSY-OUT SUMMARY     H.248 LINK SUMMARY
    Major:    0       Trunks:    0       Links Down:    0     # Logins: 2
    Minor:    0     Stations:    0         Links Up:    8
  Warning:    2

                              GATEWAY STATUS

     Alarms          Alarms          Alarms          Alarms          Alarms
 MG Mj Mn Wn Lk  MG Mj Mn Wn Lk  MG Mj Mn Wn Lk  MG Mj Mn Wn Lk  MG Mj Mn Wn
Lk
  1  0| 0| 0|up
  2  0| 0| 0|up
  3  0| 0| 0|up
  4  0| 0| 2|up
  5  0| 0| 0|up
  6  0| 0| 0|up
  7  0| 0| 0|up
  8  0| 0| 0|up
```

Table 19: The status media-gateway Command Display on page 64 describes the display associated with each section of the **`status media-gateway`** screen.

Table 19: The status media-gateway Command Display

Section	Display
ALARM SUMMARY	Current number of alarms (Major/Minor/Warning) for the total number of media gateways administered
BUSY-OUT SUMMARY	Current number of trunks/stations that are in a busy-out state for the total number of media gateways administered
H.248 LINK SUMMARY	Current number of H.248 links that are down and up for the total number of media gateways administered
GATEWAY STATUS	Number of major alarms, minor alarms, and warnings that exist, and the status of the H.248 link, either up or down (dn), on each of the media gateways administered

Hidden Communication Manager SAT commands

Certain Communication Manager SAT commands have no practical use or are not supported on an Avaya G350 Media Gateway. These commands are removed from the S8300 Media Server/LSP software to prevent any misunderstanding or confusion as to what functions are supported. The S8300 Media Server/LSP runs a subset of Communication Manager code.

Table 20: Disabled SAT Commands on page 64 through Table 22: Additional Disabled SAT Commands on page 66 can be read by using the column heading followed by the row element (e.g., add atm). Row elements with items in '()' are a third required part of the command (e.g., list configuration atm). The columns of this table are independent of each other. These commands may or may not require an argument.

Table 20: Disabled SAT Commands *1 of 2*

add	change	display	remove	list
atm	atm	atm	atm	atm
cabinet	cabinet	cabinet	cabinet	cabinet
data-module	circuit-packs	circuit-packs	data-module	configuration (atm)
fiber-link	data-module	data-module	fiber-link	configuration (carrier)

1 of 2

Table 20: Disabled SAT Commands *2 of 2*

add	change	display	remove	list
ipserver-interface	fiber-link	fiber-link	ipserver-interface	configuration (port-network)
modem-pool	ipserver-interface	ipserver-interface	modem-pool	configuration (control)
pgate	modem-pool	modem-pool	pgate	data-module
	paging (loudspeaker)	paging (loudspeaker)		fiber-link
	pgate	pgate		ipserver-interface
	synchronization	synchronization		isdnpri-testcall
	system-parameters (ipserver-interface)	system-parameters (ipserver-interface)		measurement (atm)
				measurement (clan)
				measurement (modem-pool)
				modem-pool
				pgate

2 of 2

Table 21: More Disabled SAT Commands *1 of 2*

status	set	reset	busyout/ release	test
atm	ipserver-interface	disk	atm	card-mem
cabinet	pnc	fiber-link	data-module	customer-alarm
card-mem	switch-node-clock	host-adapter	disk	data-module
clan-ip	synchronization	interface	ds1-facility	disk
clan-port	tdm	ipserver-interface	fiber-link	environment
data-module	tone-clock	maintenance	host-adapter	fiber-link
interface		packet-interface	ipserver-interface	hardware-group (cabinet)
isdnpri-testcall		pnc	modem-pool	hardware-group (carrier)
packet-interface		port_network	pnc-standby	hardware-group (pnc)
pgate-port		tone-clock	tdm	host-adapter
pnc			tone-clock	interface

1 of 2

Table 21: More Disabled SAT Commands *2 of 2*

status	set	reset	busyout/ release	test
port-network				isdnpri-testcall
switch-node				led (switch-node)
synchronization				maintenance
system				mass-storage
				modem-pool
				network-control
				packet-interface
				pkt
				synchronization
				tdm
				tone-clock
				2 of 2

Table 22: Additional Disabled SAT Commands

backup	clear	duplicate	enable/ disable	format	monitor	recycle
disk	interface	data-module	synchronization -switch	card-mem	system (conn)	carrier
	isdnpri-testcall			disk		
	pgate-port					

Note:

In addition to the commands listed above, the **`save translations`** command is disabled in the case of an S8300 configured as an LSP. For an LSP, translations are received from the primary server, and there is no need to save them.

Dynamic Call Admission Control

In order to manage the flow of calls and voice data on the G350 most efficiently, the Media Gateway Controller must have real-time information about the network topology and currently available bandwidth. Without this, changes to the network structure, such as switching over to a backup line, can cause the network to become overloaded with voice data. The MGC, unaware of the switchover, continues to admit calls at the same volume, causing network congestion. Using the Dynamic CAC (Call Admission Control) feature, the G350 can provide the MGC with up-to-date information on the bandwidth available for voice data.

By default, G350 interfaces do not participate in Dynamic CAC. However, it is highly recommended to enable Dynamic CAC on the G350's interfaces. If users report problems with long delays, jitter, and loss of calls, enable Dynamic CAC to provide greater link reliability and robustness.

Enabling Dynamic CAC on the G350

Use the **dynamic-cac** command to enable Dynamic CAC on the G350. Dynamic CAC must be enabled on each interface responsible for providing call bandwidth. If Dynamic CAC is enabled on more than one interface, specify an activation priority for each interface. The BBL (Bearer Bandwidth Limit) is reported as the BBL of the interface with the highest activation priority.

The dynamic-cac command has the following syntax:

dynamic-cac ***bbl*** [***activation-priority***]

Using Dynamic CAC on the Media Gateway Controller

Use the **change ip-network-region** SAT command to mark direct connections among regions as "**:Dynamic**", and specify which media gateway is responsible for setting dynamic CAC updates for that link.

Use the **status ip-network-region** SAT command to view the current dynamic bandwidth value.

System resets

There is no change in how Communication Manager functions for system resets in Avaya S8300 Media Server with a media gateway. Although translations may be present for a media gateway, Communication Manager waits for a link to be established before attempting to access the media gateway. Upon notification that registration has occurred, maintenance waits for the Media Module Manager to indicate that a Media Module is present before attempting to determine which Media Modules are present.

In the event of a media gateway power failure or loss of signaling, Communication Manager detects that the media gateway is no longer registered and, after certain conditions are satisfied, begins to remove Media Modules (see H.248 server-to-gateway Link Recovery on page 69).

For Media Server resets (as opposed to media gateway resets) the media gateway attempts to re-register with the same server, and if not successful attempts to find another Media Server. When a Media Server is found, the Media Module discovery process ensues.

Audits

The Communication Manager audit that verifies board presence runs in order to detect missing Media Modules after system initialization. As a result, the media gateway is audited to verify that all boards that were originally present are still present after a reboot.

Automatic launch of Traceroute (ALT)

Note:

Currently, this feature operates exclusively on the S8300 Media Server.

When an Avaya G350 Media Gateway unregisters from the S8300 Media Server, the server platform automatically sends a request to the server to execute a **`traceroute`** command. The Linux program **`traceroute`** is used to probe the IP address of the media gateway. In this way, if a LAN component has failed, the **`traceroute`** command will discover the component. A log is kept on the platform, and can be viewed with the Linux command **`trrtelog`**.

In order to keep from overloading platform processes, a traceroute cannot be executed in less than 10 seconds from the last command. The maximum rate that traceroute can be run is therefore no more than six per minute. If the customer does not want this capability, it can be turned off by a technician. The flag “trrte_run” is set to zero to disable the automatic execution of the command.

Results Evaluation

The technician determines the time of the media gateway outage and then reads the ALT log to find a similar time. If a trace had been executed, the technician verifies that the IP addresses are the same. If there is no matching IP address, there may be other addresses representing other Media Gateways on the same subnet. In this case, the log entries may still be useful in tracking down a potential source of trouble.

H.248 server-to-gateway Link Recovery

The H.248 link between an Avaya server running Avaya Communication Manager Software and the Avaya Media Gateway provides the signaling protocol for:

- Call setup
- Call control (user actions such as Hold, Conference, or Transfer) while the call is in progress
- Call tear-down

If the link goes down, Link Recovery preserves any existing calls and attempts to re-establish the original link. If the gateway cannot reconnect to the original server, then Link Recovery automatically attempts to connect with another server or Local Spare Processor (LSP). Link Recovery does not diagnose or repair the network failure that caused the link outage.

The main Link Recovery topics are:

- Applicable hardware and adjuncts
- Conditions that trigger link recovery
- Link recovery processes
  - General link recovery process
  - Call handling during recovery
  - Maintenance during recovery
- Link recovery administration
  - Administering the server timer
  - Administering the Media Gateway

Applicable hardware and adjuncts

Link Recovery is compatible with:

- Avaya Communication Manager Release 2.0
- Avaya S8300/S8500/S8700 Media Server with Avaya G350 Media Gateway and Avaya Media Modules and all applicable endpoints

Note:

The software and firmware versions on the server and the gateway must match (Release 1.3). If they do not match, the intent of Link Recovery is circumvented because the gateway resets (drops calls) as soon as the link loss is detected.

Conditions that trigger link recovery

Link Recovery begins with detection of either:

- A TCP socket failure on the H.248 link

  or

- Loss of the H.248 link within 40-60 seconds

Link recovery processes

This section describes the Link Recovery scenarios and the concurrent call handling and maintenance activities:

- General link recovery process
- Call handling during recovery
- Maintenance during recovery
- Link recovery unsuccessful

General link recovery process

Link Recovery design incorporates three separate timers that monitor the period of time that the server or gateway spends in specific Link Recovery processes. Table 23: Link Recovery Timers on page 71 lists the timer parameters.

Table 23: Link Recovery Timers

Timer	Location	Description	Value range in minutes (default)
Link Loss Delay Timer	Server	The length of time that the server retains call information while the gateway attempts to reconnect to either its primary server or to alternate resources.	1-30 (5)
Primary Search Timer	Gateway	The length of time that the gateway spends trying to connect to the primary server.	1-60
Total Search Timer	Gateway	The length of time that the gateway spends trying to connect to all alternate resources.	1-60

The sequence of events during Link Recovery is described in Table 24: General Link Recovery process on page 71.

Table 24: General Link Recovery process *1 of 2*

Process sequence	Description
1.	Link failure detected (see Conditions that trigger link recovery on page 70)
2.	The Primary and Total Search Timers begin running. The gateway attempts to re-establish the H.248 link with original server, which is the first element in the Media Gateway Controller (MGC) list. See Administering the MGC list on page 77 for instructions on administering this list. See Administering the gateway timers and Transition Point on page 77 for instructions on administering the Primary and Total Search Timers.

1 of 2

Table 24: General Link Recovery process *2 of 2*

Process sequence	Description
3.	If the gateway cannot reconnect with the original server, then it searches the MGC list (in order) for alternate resources (list elements 2-4) that are above the Transition Point (if set). These alternate resources can be: 1. **S8300**: 1-3 S8300s configured as Local Spare Processors (LSPs) 2. **S8700**: 1-3 C-LAN circuit packs within the primary server's configuration The Total Search Timer continues running. See Administering the MGC list on page 77 for instructions on administering this list and setting the Transition Point.
4.	If the Primary Search Timer expires before the gateway can re-establish the link to the alternate resources that are above the Transition Point in the MGC list, then the gateway crosses the Transition Point and begins searching the other resources in the list. The gateway makes only one connection attempt with any resources below the Transition Point.
5.	If the gateway cannot re-establish the link to any of the resources below the Transition Point, then it starts over at the top of the MGC list and continues to the end, making only one reconnection attempt to each element in the list. This continues until the Total Search Timer expires.
6.	If the gateway still cannot connect to any alternate resources and Total Search Timer expires, the software raises a warning alarm. See Maintenance during recovery on page 73 for more information about the server and gateway alarm notification strategies. The server's Link Loss Delay Timer should be the last timer to expire, meaning that the server holds its call control information until all other means of re-establishing the link have been exhausted. **Note:** If the Link Loss Delay Timer expires but the gateway successfully connects with an alternate resource, the system generates a warning alarm anyway, even though the H.248 link is up.
	2 of 2

Call handling during recovery

While the H.248 link is down, calls that were already in progress before the link failure remain connected during the recovery process. Once the link is re-established, normal call processing continues. If the gateway successfully reconnects, the actual outage is less than 2 seconds. Should the link failure persist for a few minutes, some features or capabilities are affected:

- New calls are not processed.
- Calls held in queue for an attendant group, call park, or calls on hold might be dropped during Link Recovery.
- The talk path between two or more points remains up, even if one or all of the parties hangs up.
- Music or announcement sources associated with a call remain connected to queued or held calls in progress, even if one or all parties to the call hangs up.
- If the link failure continues for several minutes, expect inaccuracies in the BCMS, CMS, call attendants, and other time-related statistical reports.
- If the calling party hangs up during Link Recovery, expect inaccuracies in the CDR records for the recovery time period.
- Phone buttons (including feature access buttons) do not work.

The Feature interactions and compatibility on page 78 section describes other performance impacts associated with Link Recovery.

Maintenance during recovery

During Link Recovery the following maintenance events occur:

- If a Media Module change occurs during the link failure but before the expiration of the Total Search Time, the gateway informs the controller of the change after the link is re-established.
- Any Media Modules that were reset, removed, or replaced are removed and inserted in Communication Manager.
- The maintenance subsystem begins a context audit after Link Recovery.

Link recovery unsuccessful

If link recovery was unsuccessful, both Communication Manager and the media gateway generate events and alarms.

Server alarms

Expiration of the Link Loss Delay Timer triggers Communication Manager alarm notification. These events and their associated alarm levels are in Table 25: Avaya Communication Manager alarms on page 74.

Table 25: Avaya Communication Manager alarms

Event	Alarm level
Link Loss Delay Timer expires (loss of link to gateway)	Minor
Gateway reconnects	Clear
Original gateway fails to reconnect	Major
Original gateway reconnects	Clear

Gateway alarms

The Media Gateway events, their associated alarm levels, and SNMP status are listed in Table 26: Media Gateway events and alarms on page 74.

Table 26: Media Gateway events and alarms

Event	Alarm level	Log	SNMP
Loss of link	Major	event	trap
Link restored	Major	event	trap clear
Registration successful	Informational	event	trap
Registration failed	Major	event	trap
No controller provisioned	Major	event	trap
Controller provisioned	Major	event	trap clear
Connection to LSP	Major	event	trap
Connection fallback to primary	Major	event	trap clear

Note:

Avaya Communication Manager does not raise an alarm until the Link Loss Delay timer expires. If the link to the original gateway is restored before this timer expires, then no alarm is raised.

If the Link Loss Delay Timer expires but the gateway successfully connects with an LSP, Avaya Communication Manager generates a warning alarm anyway, even though the H.248 link is up.

Link recovery administration

Link Recovery requires both Avaya Communication Manager and Media Gateway administration. Link Recovery administration involves:

- Administering the server timer
- Administering the Media Gateway
  - Administering the gateway timers and Transition Point
  - Administering the MGC list

Administering the server timer

The Link Loss Delay Timer determines how long Communication Manager retains the gateway's call state information before it instructs the gateway to reset, dropping all calls in progress.

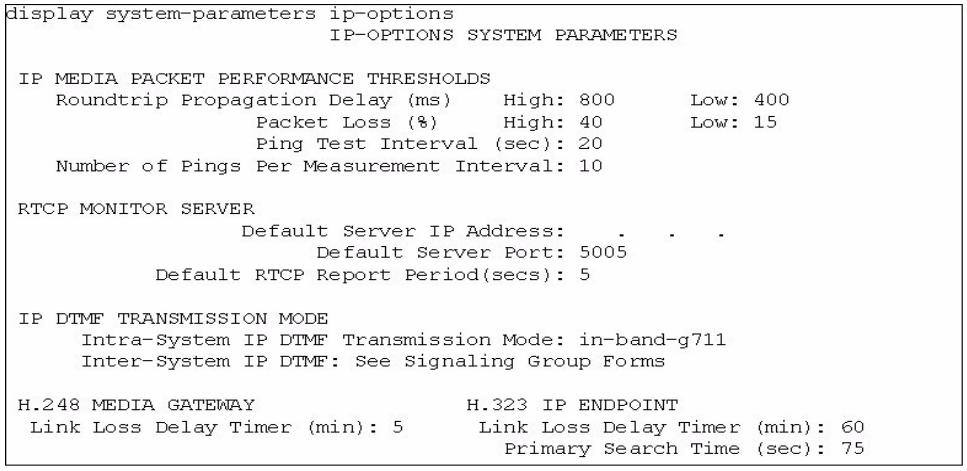
To administer the Link Loss Delay Timer:

1. At the SAT prompt, type **`change system-parameters ip-options`** and press **Enter** to display the system parameters ip-options form (Figure 9: System-parameters ip-options form on page 76).
2. In the H.248 MEDIA GATEWAY section type a number (**1**-**30**; default is **5**) in the `Link Loss Delay Timer (minutes)` field. This is the number of minutes that Communication Manager retains the gateway's call state information.

   Note:

   The value of this timer should be longer than either of the gateway timers (see Administering the gateway timers and Transition Point on page 77).
3. Press **Enter** to save the change.

Figure 9: System-parameters ip-options form



```
display system-parameters ip-options
                        IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS
   Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                   Packet Loss (%)     High: 40       Low: 15
                   Ping Test Interval (sec): 20
   Number of Pings Per Measurement Interval: 10

RTCP MONITOR SERVER
                  Default Server IP Address:    .   .   .
                        Default Server Port: 5005
           Default RTCP Report Period(secs): 5

IP DTMF TRANSMISSION MODE
     Intra-System IP DTMF Transmission Mode: in-band-g711
     Inter-System IP DTMF: See Signaling Group Forms

H.248 MEDIA GATEWAY                 H.323 IP ENDPOINT
 Link Loss Delay Timer (min): 5      Link Loss Delay Timer (min): 60
                                       Primary Search Time (sec): 75
```

IP-Options Form Fields

The **`display system-parameters ip-options`** screen contains the following information:

- **IP Media Packet Performance Thresholds** – used to determine the quality of the network between various network regions and systems. If the network is judged to be of poor quality based on these parameters, Communication Manager attempts to route calls via a different path (e.g., PSTN).
- **RTCP Monitor Server** – a server that collects all RTCP information
- **IP DTMF Transmission Mode** – indicates whether to send DTMF tones in band or out of band
- **H.248 Media Gateway Link Loss Delay Timer** – the amount of time that a media gateway waits before attempting to register with another controller after losing its link to the current controller. If it regains a connection to the primary controller within that time, calls that were active when the link was lost remain active.
- **H.323 IP Endpoint Link Loss Delay Timer** – similar to the previous field
- **H.323 IP Endpoint Primary Search Timer** – amount of time an H.323 endpoint should keep trying to register with its primary controller before moving to an LSP

Administering the Media Gateway

Administering the Media Gateway requires you to administer the Primary Search Timer, the Total Search Timer, and the MGC list Transition Point. You also administer an MGC list of up to four alternate controllers for the gateway.

Administering the gateway timers and Transition Point

To administer the gateway timers and Transition Point

1. Administer the gateway's **Primary Search Timer** (the length of time that the gateway spends trying to connect to the primary server) by typing **`set reset-times primary-search <search-time>`** at the Command Line Interface (CLI). The <*search-time*> values are **1-60** minutes.

   Note:

   The Primary Search Timer value should be shorter than both the Total Search Timer and the Link Loss Delay Timer.

2. Save the configuration changes using the **`copy running-config startup-config`** command.

3. Administer the **Total Search Timer** (the length of time that the gateway spends trying to connect to all alternate resources) by typing **`set reset-times total-search <search-time>`** at the Command Line Interface (CLI). The <*search-time*> values are **1-60** minutes.

   Note:

   The Total Search Timer value should be greater than the Primary Search Timer but shorter than the Link Loss Delay Timer.

4. Establish the **Transition Point** (in either of the previous steps) by typing **`set reset-times transition-point <n>`**, where **`<n>`** is the numbered element in the MGC list.

   For example, if n= 2, the Transition Point is after the second element in the list. That is, the gateway first attempts reconnecting with its original C-LAN circuit pack and then tries one other alternate resource during the Primary Search Timer period. See Table 23: Link Recovery Timers on page 71 for more information about the Link Recovery timers.

Administering the MGC list

You can administer the gateway with a list of up to 4 alternate resources (TN799DP C-LAN circuit packs or LSPs) that it can connect to in the event of link failure. The MGC list consists of the IP addresses to contact and the order in which to re-establish the H.248 link.

To administer the MGC list:

1. At the gateway's Command Line Interface (CLI) type **`set mgc list <ipaddress>, <ipaddress>,<ipaddress>,<ipaddress>`**, where:

   - The first element is the IP address of the primary server (S8300) or the primary C-LAN circuit pack (S8700).
   - The next three elements are the IP addresses of 1-3 LSPs (S8300s configured as such) or of any other C-LAN circuit packs in the primary server's configuration (S8700).

   There are a total of four elements in this list.

2. Reset the gateway by typing **reset**.

   Wait for the LEDs on the gateway and Media Modules to go out and the active status LEDs on the gateway to go on, indicating that the reset is complete.

3. Check the MGC list administration by typing **show mgc list**.

   Look in the CONFIGURED MGC HOST section of the output for the IP addresses of the alternate resources.

Feature interactions and compatibility

H.248 Link Recovery can affect the performance of features or adjuncts within the configuration (Table 27: H.248 Link Recovery feature/adjunct interactions on page 78).

Table 27: H.248 Link Recovery feature/adjunct interactions *1 of 2*

Feature or adjunct	Description
Feature Access Codes (FAC)	Feature Access Codes, whether dialed or administered buttons, do not work.
Non-IP trunks/stations, including such circuit-switched TDM resources as DCP, analog, or ISDN-PRI	These resources are unavailable until the H.248 link is re-established.
Terminals	Time-of-Day, busy lamp states, and call appearance status on some phones might not instantaneously reflect the correct information until the H.248 link is re-established.
Adjunct Switch Application Interface (ASAI)	ASAI-based applications that utilize timing loops, time-related methods, or events might not perform as intended. In addition, applications that do not accommodate time-outs or missing state transition(s) might behave unpredictably.
Voice mail adjuncts (INTUITY, INTUITY Audix)	During Link Recovery, callers connected to AUDIX remain connected even if they hang up. Such calls might be automatically disconnected by AUDIX if the connection remains intact without the calling party entering tone commands to AUDIX or voicing a message.
Call Detail Recording (CDR)	Call records cannot reflect the correct disconnect time if the calling party hangs up before the link recovers.
Call Management System (CMS)	Measurements collected during the recovery period might be inaccurate in those reports that rely upon time-related data.

1 of 2

Table 27: H.248 Link Recovery feature/adjunct interactions *2 of 2*

Feature or adjunct	Description
Property Management System (PMS)	Automatic Wake-up, Daily Wake-up, and Housekeeping Status features might not operate as expected if the link fails and the time to search for alternate resources exceeds the PMS application's time-out parameters. For example, if a guest has a wake-up call schedule for 6:15 AM and the H.248 link goes down at 6:10 but recovers at 6:20, then the guest receives no wake up call at 6:15.
Conversant voice response systems	Conversant applications that utilize timing loops, time-related methods, or events might not perform as intended. In addition, applications that do not accommodate time-outs or missing state transition(s) might behave unpredictably.
	2 of 2

Network Fragmentation

A likely outcome to an H.248 link recovery scenario is that a network of media gateways and IP endpoints, initially registered to the primary server, may now be registered to a number of different LSPs in the network. This can be very disruptive in that network capability may be highly compromised. Resources at various points in the network may be available in only limited quantities, or not at all.

The SAT commands **`list media-gateway`** and **`status media-gateway`** can show those network elements that are not registered with the primary server. If the technician is on site, the illumination of the YELLOW ACT LED on the LSP is an indication that something has registered with that LSP, and therefore, that the network is fragmented. At the present time, two methods are available to recover from a fragmented network:

- Use the S8300 Web Interface to shut down each LSP
- Execute **`reset system 4`** on each LSP
- Shut down Communication Manager on every LSP

Use the S8300 Web Interface

You can use the S8300 Web Interface to shutdown and reboot each LSP registered with the server. This is the recommended way for customers to reestablish the LSP's connection to the primary server.

Execute reset system 4

In order to force Media Gateways and IP endpoints to re-register with the primary server, execute a **reset system 4** command on each media gateway containing an LSP, thus forcing any media gateways and IP endpoints registered to the LSP to search for and re-register with the primary server. The expectation is that these endpoints will correctly perform the search and find the primary server; however, there is no guarantee that this will be the result.

Shut down Communication Manager on every LSP

The only way to be certain that media gateways and endpoints re-register with the primary server is to shut down Communication Manager on every LSP in the network, using the Linux command **stop -acfn**. Afterward, the primary server SAT commands **list media-gateway** or **status media-gateway** can verify whether all the network endpoints re-registered with the primary server. The Linux command **start -ac** sent to each LSP will then restart Communication Manager on each of those platforms.

Maintenance Objects

The maintenance subsystem is partitioned into separate entities called Maintenance Objects (MOs). A maintenance object can be:

- An individual Media Module
- A hardware component that is part of a Media Module
- An entire subsystem
- A set of monitors
- A process (or set of processes)
- A combination of processes and hardware

“Maintenance names” are recorded in the Error and Alarm logs. Individual copies of an MO are assigned an address that defines the MO’s physical location in the system when applicable. These locations display as the **port** field in the Alarm and Error logs and as output of various commands such as **test board** (see Figure 10: Display of test board command on page 81).

Figure 10: Display of test board command

```
test board 1v4 long                                              Page   1

                                TEST RESULTS

Port        Maintenance Name  Alt. Name  Test No.  Result        Error Code

001V4       MG-DS1                       50        ABORT         1412
001V4       MG-DS1                       52        PASS
001V4       MG-DS1                       138       PASS
001V4       MG-DS1                       139       PASS
001V4       MG-DS1                       140       PASS
001V4       MG-DS1                       141       PASS
001V4       MG-DS1                       142       PASS
001V4       MG-DS1                       143       PASS
001V4       MG-DS1                       144       PASS
001V4       MG-DS1                       145       PASS
001V4       MG-DS1                       146       PASS
001V4       MG-DS1                       1227      ABORT         1412
001V401     TIE-DS1           0001/001   7         ABORT         1412
```

Avaya G350 Media Gateway MOs

The following list shows new, G350 specific maintenance objects. Other maintenance objects have been modified slightly for the G350.

- MED-GTWY (MEDIA GATEWAY)
- MG-ANA (ANALOG MM711, MM714)
- MG-BRI (BRI Trunk Media Module MM720 and MM722)
- MG-DCP (Digital Line Media Module)
- MG-DS1 (DS1 Interface Media Module)
- MG-ICC (Internal Call Controller)
- MG-VAMM (G350 integrated analog module in V7)

Note:

Data modules are not tested by the maintenance objects.

MO groupings by MM type

Table 28: Media Module Tests on page 82 shows MO groupings by Avaya Media Module type.

Table 28: Media Module Tests *1 of 2*

Media Module	Maintenance Object
T1/E1 Media Module	Board (MG-DS1)
	DS1 CO Trunk (CO-DS1)
	DS1 DID Trunk (DID-DS1)
	DS1 Tie Trunk (TIE-DS1)
	DS1 ISDN Trunk (ISDN-TRK)
	ISDN-PRI Signaling Link Port (ISDN-LNK)
	ISDN-PRI Signaling Group (ISDN-SGRP)
	Wideband Access Endpoint Port (WAE-PORT)
Analog Media Module	Board (MG-ANA)
	Analog Line (AN-LN-PT)
	Analog Co Trunk (CO-TRK)
	Analog DID Trunk (DID-TRK)
	DIOD Trunk (DIOD-TRK)
	Alarm Port (ALARM-PT)
DCP Media Module	Board (MG-DCP)
	Digital Line (DIG-LINE)

1 of 2

Table 28: Media Module Tests *2 of 2*

Media Module	Maintenance Object
BRI Trunk Media Module	Board (MG-BRI)
	ISDN Trunk Side BRI Port (TBRI-PT)
	ISDN Trunk Side Signaling (TBRI-TRK)
Integrated Analog Module in V7	MG-VAMM
	2 of 2

MO test commands

Each command is arranged according to a standard command syntax for Avaya G350 Media Gateways, where GGG is the G350 Number, the character V indicates that this system is a G350, S is the slot number, and PP is the port number.

Full test commands can be either short or long as indicated, and can be repeated several times. For example, in:

`test port GGGVSpp sh r 1`

sh = short

r = repeat

1 = the number of times the test should be repeated.

Similarly, in:

`test port GGGVSpp l r 2`

l = long

r = repeat

2 = the number of times the test should be repeated.

Abort Code 1412

Tests that do not run on the G350 will abort with Abort Code 1412. Tests that abort are listed under each MO, but are not described.

ALARM-PT (ALARM PORT)

Table 29: ALARM-PT (ALARM PORT)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run	Full Name of MO
ALARM-PT	MIN	test port GGGVSPP l	Alarm-Port
ALARM-PT	WRN	test port GGGVSPP sh	Alarm-Port
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			

The Alarm Port MO provides on-board maintenance for an analog line port that is administered as an external device alarm port. Test are provided to verify the analog line port's ability to detect an external device alarm. The external device alarm (EXT-DEV) MO is used for the off-board external device alarm.

Error Log entries and Test to Clear values

Table 30: 8-Port Analog Line Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port GGGVSpp sh r 1
15 (a)	Any	Audits and Updates Test (#36)			

1 of 2

Table 30: 8-Port Analog Line Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
18	0	busy-out station *extension*	WARNING	OFF	release station *extension*
130 (b)		None	WARNING	ON	test port GGGVSpp sh
769		Battery Feed Test (#35)	MINOR	ON	test port GGGVSpp sh r 2
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					

Notes:
(a) This is a software audit error that does not indicate any hardware malfunction. Run Short Test SeSquence and investigate errors.
(b) Indicates that the Media Module has been removed or has been insane for more than 11 minutes. To clear the error, reset or replace the Media Module.

2 of 2

System technician-demanded tests: Descriptions and Error Codes

CAUTION:
Always investigate tests in the order presented in the table below. By clearing error codes associated with the *Battery Feed Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 31: System Technician-Demanded Tests

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
Battery Feed Test (#35)	X	X	ND
Station Status and Translation Audits and Updates Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Battery Feed Test (also called Port Diagnostic Test) (#35)

The battery feed chip provides power to the telephone equipment, signaling, rotary dial pulsing, transmission, and balance. This test checks the signaling and switchhook capabilities of the battery feed chip by terminating the port, applying battery, and trying to detect a current.

Table 32: TEST #35 Battery Feed Test

Error Code	Test Result	Description/Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be reporting an external device alarm. Enter **test external-device-alarm port GGGVSpp** to determine if the port is reporting an EXT-DEV failure before retesting. When the port has no EXT-DEV failure, retry the command at 1-minute intervals for a maximum of 5 times.
1004	ABORT	The port received an EXT-DEV failure during the test. The test has been aborted. Enter **test external-device-alarm port GGGVSpp** to determine if the port is reporting an EXT-DEV failure before retesting. If the port has no EXT-DEV failure, retry the command at 1-minute intervals for a maximum of 5 times.
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	The port's battery feed chip is unable to supply sufficient power to sense the external device alarm. This may occur when the test is performed at the same time that the external device contact closure occurred. Enter **test external-device-alarm port GGGVSpp** to determine if the port is reporting an EXT-DEV failure before retesting. Wait until the port has no EXT-DEV failure before retesting. Retry the command at 1-minute intervals for a maximum of 5 times.
	PASS	The port's battery feed chip is able to provide power to the external device alarm to detect contact closure.

Station Status and Translation Audits and Updates Test (#36)

For an analog line port that is administered as an external alarm, this test is limited to updating the software with the switchhook state.

Table 33: TEST #36 Station Status and Translation Audits and Updates

Error Code	Test Result	Description/Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1004	ABORT	The port received an EXT-DEV failure during the test. The test has been aborted. Enter **test external-device-alarm port GGGVSpp** to determine if the port is reporting an EXT-DEV failure before retesting. If the port has no EXT-DEV failure, retry the command at 1-minute intervals for a maximum of 5 times.
1006	ABORT	This port has been busied out by command. Check Error Log for Error Type 18 (port busied out). If present, release the port with the **release port** command and run the test again.
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1	FAIL	This failure does not indicate a hardware problem. The switchhook audit failed, this condition may occur when the audit is performed at the same time that the terminal equipment goes off-hook. Enter test external-device-alarm port GGGVSpp to determine if the port is reporting an EXT-DEV failure before retesting. Wait until the port has no EXT-DEV failure before retesting If the port has no EXT-DEV failure, retry the command at 1-minute intervals for a maximum of 5 times.
7	FAIL	The translation update failed. This does not indicate a hardware problem but may be an internal software error.
	PASS	The software and the port processor have the same status.

AN-LN-PT (Analog Line Port)

Table 34: AN_LN_PT (Analog Line Port)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
AN-LN-PT	MIN	test port GGGVSPP	Analog Line Port
AN-LN-PT	WRN	test port GGGVSPP	Analog Line Port
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			

The MM711 Analog Trunk and Line Media Module provides 8 ports, each of which may be administered in any of several ways, as described in maintenance object MG-ANA.

Ringing caused by maintenance testing

Test #48 may cause some terminal equipment to ring briefly during daily maintenance. If this ringing disturbs the customer or the terminal equipment, disable it in the `Tests` field of the **change station *extension*** form. Be aware that this action also disables Tests #6, 7, and 35 on some software releases.

Error log entries and Test to Clear values

Table 35: Analog Line Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port GGGVSpp sh r 1
1(a)	40960 40975 40977	none			
15(b)	Any	Audits and Updates Test (#36)			

1 of 2

Table 35: Analog Line Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
18	0	busy station *extension*	WRN	ON	release station *extension*
130(c)		None	WRN	ON	test port GGGVSpp sh
257(d)	40973	none			
513(e)		Station Present Test (#48)	WRN	OFF	test port GGGVSpp sh r 2
769		Battery Feed Test (#35)	MIN/ WRN**	ON	test port GGGVSpp sh r 2

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

Minor alarms on this MO may be downgraded to Warning alarms based on the values used in the **set options command.

2 of 2

Notes:

- **(a) Error Type 1** - these in-line errors can only be resolved over time:
  - Aux Data 40960 indicates that too many simultaneous incoming ringing attempts were made on this board. Only 4 ports on a board may ring simultaneously. A 5th incoming call will cause an inline error from the board.
  - Aux Data 40975 indicates that the terminal equipment was on-hook when ring-tip was detected during ringing. This usually indicates a failure in the terminal equipment or the type of terminal has a low ringer impedance.
    - Call the terminal equipment and verify that the terminal rings.
    - If the terminal does not ring, then replace it.
    - Otherwise, use the **test port GGGVSpp** command, and follow the procedure for Test #48.
  - 40977 indicates that no terminal equipment was connected when ringing was attempted.
    - Run the short test via the **test port GGGVSpp** command, and follow the procedure for the results of Test #48.
- **(b) Error Type 15** - a software audit error that does not indicate any hardware malfunction
  - Run the Short Test Sequence and investigate any associated errors.

- **(c) Error Type 130** - indicates that the Media Module has been removed or has been insane for more than 11 minutes
  - To clear the error, reset or replace the Media Module.
- **(d) Error Type 257** - an in-line error that can only be resolved over time. This error indicates that ringing voltage is absent
  - If not resolved over time, replace the module.
- **(e) Error Type 513** - Test #48 can cause some terminal equipment to ring briefly during daily maintenance.
  - If this disturbs the customer or the terminal equipment, disable it by setting the `Tests` field on the **change station *extension*** form to **n**. This may also disable Test #35.

System Technician-Demanded Tests: Descriptions and Error Codes

CAUTION:

Always investigate tests in the order presented in the table below when inspecting errors in the system. By clearing error codes associated with the *Battery Feed Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 36: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
Battery Feed Test (#35)	X	X	ND
Station Present Test (#48)	X	X	ND
Looparound Test (#161) **Note:** *This test will abort with Error Code 1412.*		X	ND
Conference Test (#7) **Note:** *This test will abort with Error Code 1412.*		X	ND
NPE Crosstalk Test (#6) **Note:** *This test will abort with Error Code 1412.*		X	ND
Station Status and Translation Audits and Updates Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Battery Feed Test (also called Port Diagnostic Test) (#35)

The battery feed chip provides power to the telephone equipment, signaling, rotary dial pulsing, transmission, and balance. This test checks the signaling and switchhook capabilities of the battery feed chip by terminating the port, applying battery power, and detecting the resulting current.

Table 37: TEST #35 Battery Feed Test *1 of 3*

Error Code	Test Result	Description/Recommendation
	ABORT	Necessary system resources could not be allocated to run this test. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1000	ABORT	System resources are unavailable. The port may be busy with a valid call. This result is also reported for the system's Music-On-Hold port when it is off-hook, which it usually is. Enter **display port GGGVSpp** to determine the station's extension. Enter **status station *extension*** to determine the service state of the port. If the port is in use, wait until the port is idle. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1004	ABORT	A valid call seized the port during the test and aborted the test. Use the **display port GGGVSpp** command to determine the station extension. Use the **status station *extension*** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1005	ABORT	This test was aborted due to a configuration problem. The test is not applicable for this type of analog port. This error can be ignored.
1018	ABORT	Administration has disabled the test. The default for the `Test?` field on the station form is **y**. Determine why this field has been set to **n** on this station (this may be due to the ringing application Test #48, which can be disturbing to customer or terminal equipment). To enable the test for a particular station being tested, enter **change station *extension***. Change the `Test?` field on the station form to **y**.

1 of 3

Table 37: TEST #35 Battery Feed Test *2 of 3*

Error Code	Test Result	Description/Recommendation
1392	ABORT	This port is currently a TTI port and the test does not execute on it. Verify that the port is a TTI port: Enter the **display port GGGVSpp** command (the display shows that the port is a TTI port). Enter the **list configuration** command (the display shows a **t** for the port). If both commands indicate that the port is a TTI port, the abort is correct for the test, and no action is necessary. If either command indicates that the port is *not* a TTI port, escalate the problem.
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	System resources required to run this test are not available. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
	FAIL	The port's battery feed chip is unable to supply sufficient power to the terminal equipment. This test result might be marginal, and the terminal equipment may be operating satisfactorily. Retry the command at 1-minute intervals no more than 5 times. If the test continues to fail, determine whether the customer is experiencing problems on this line. Replace the Media Module only if the customer is experiencing problems.

2 of 3

Table 37: TEST #35 Battery Feed Test *3 of 3*

Error Code	Test Result	Description/Recommendation
	PASS	The port's battery feed chip is able to provide sufficient power to the station equipment to detect on-/off-hook, but may not be able to supply power for touch-tones. If touch-tones are inoperative on this station, replace the Media Module because this port is inoperative. Investigate user-reported troubles on this port by running other port tests, by examining station wiring, or by inspecting the station.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This result could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Check to make sure that the board translations are correct. Use the **list configuration** command, and resolve any problems. If the board is correctly inserted, use the **busy board GGGVS** command. Use the **reset board GGGVS** command. Use the **release board GGGVS** command. Use the **test board GGGVS long** command. This re-establishes the link between the internal ID and the port. If this is not the case, check to make sure that a valid board is inserted.

3 of 3

Station Status and Translation Audits and Updates Test (#36)

This test updates the analog port's message lamp state (if it has one) and translations with information in the software.

Table 38: TEST #36 Station Status and Translation Audits and Updates *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Necessary system resources could not be allocated to run this test. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1004	ABORT	A valid call seized the port during the test and aborted the test. Use the **display board GGGVSpp** command to determine the station extension. Use the **status station *extension*** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1005	ABORT	This test was aborted due to a configuration problem. The test is not applicable for this type of analog port. This error can be ignored.
1006	ABORT	The port is out-of-service. The **busy station *extension*** command has been given to this port. Look for error type 18 (port busied out) for this port. If this error is present, release the port (**release station *extension***), and run the test again. Make sure that the terminal is connected and in service, and then retest.
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	System resources required to run this test are not available. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.

1 of 2

Table 38: TEST #36 Station Status and Translation Audits and Updates *2 of 2*

Error Code	Test Result	Description/ Recommendation
1	FAIL	The switchhook audit failed. This result does not indicate a hardware problem. The other updates were not performed because of this failure. This may occur if the audit is performed at the same time the terminal equipment goes off-hook. Use the **status station *extension*** command to determine when the port is available. Retry the command at 1-minute intervals no more than 5 times. If the test continues to fail, escalate the problem.
5	FAIL	The message waiting lamp update failed. This may be an internal software error. The translation and ringer updates were not performed because of this failure.
7	FAIL	The translation update failed. There may be an internal software error. The ringer update was not performed because of this failure.
8	FAIL	The ringer update failed. There may be an internal software error. Retry the command at 1-minute intervals no more than 5 times. If the test continues to fail, escalate the problem.
	PASS	The software and the port processor have the same status. Investigate user-reported troubles on this port by running other port tests, by examining station wiring, or by inspecting the station.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This result could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Check to make sure that the board translations are correct. Use the **list configuration** command, and resolve any problems. If the board is correctly inserted, use the **busy board GGGVS** command. Use the **reset board GGGVS** command. Use the **release board GGGVS** command. Use the **test board GGGVS long** command. This re-establishes the link between the internal ID and the port. If this is not the case, check to make sure that a valid board is inserted.

2 of 2

Station Present Test (also called Ringing Application Test) (#48)

This test applies momentary ringing voltage to the terminal equipment and monitors resulting current flow to determine whether terminal equipment is connected to the port. This test may cause some terminal equipment to ring briefly during daily maintenance. If this ringing disturbs the customer or the terminal equipment, you can disable it via the `Tests` field on the **change station *extension*** form. However, on some software releases, Tests #6, 7, and 35 also are disabled.

Table 39: TEST #48 Station Present Test *1 of 3*

Error Code	Test Result	Description/Recommendation
	ABORT	Necessary system resources could not be allocated to run this test. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1000	ABORT	System resources are unavailable. The port may be busy with a valid call. This result is also reported for the system's Music-On-Hold port when it is off-hook, which it usually is. Enter **display port GGGVSpp** to determine the station's extension. Enter **status station *extension*** to determine the service state of the port. If the port is in use, wait until the port is idle. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1004	ABORT	A valid call seized the port during the test and aborted the test. Use the **display port GGGVSpp** command to determine the station extension. Use the **status station *extension*** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
1005	ABORT	This test was aborted due to a configuration problem. The test is not applicable for this type of analog port. This error can be ignored.
1008	ABORT	A ringing circuit could not be allocated. Retry the command at 1-minute intervals no more than 5 times. Check for Error Type 257 in the hardware error log. Resolve, if present.

1 of 3

Table 39: TEST #48 Station Present Test *2 of 3*

Error Code	Test Result	Description/Recommendation
1018	ABORT	Administration has disabled the test. The default for the `Test?` field on the station form is **y**. Determine why this field has been set to **n** on this station (this may be due to the ringing application Test 48, which can be disturbing to customer or terminal equipment). To enable the test for a particular station being tested, enter **change station *extension***. Change the `Test?` field on the station form to **y**.
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	System resources required to run this test are not available. Retry the command at 1-minute intervals no more than 5 times. If the test continues to abort, escalate the problem.
	FAIL	The terminal equipment is not connected to the Media Module. Some terminal equipment, such as modems, may fail even when connected properly. Remotely test the terminal equipment. If the test fails again, resolve any RING-GEN errors in the error log, if present. Check all of the wiring between the station equipment and the switch. Then, run the test again. Some terminal equipment might fail even when it is connected properly. If this is the case, disable the test using the **change station *extension*** command (enter **n** into the `Test` field). **Note** that this action also disables Test #35 on this port. If the test still fails, the terminal equipment may be defective. Check and replace it, if necessary.

2 of 3

Table 39: TEST #48 Station Present Test *3 of 3*

Error Code	Test Result	Description/Recommendation
	PASS	The station is connected properly to the switch. Investigate user-reported troubles on this port by running other port tests, by examining station wiring, or by inspecting the station. This test may also pass if no terminal equipment is connected and the terminal is located very far from the switch.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This result could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Check to make sure that the board translations are correct. Use the **list configuration** command, and resolve any problems. If the board is correctly inserted, use the **busy board GGGVS** command. Use the **reset board GGGVS** command. Use the **release board GGGVS** command. Use the **test board GGGVS long** command. This re-establishes the link between the internal ID and the port. If this is not the case, check to make sure that a valid board is inserted.

3 of 3

CO-DS1 (DS1 CO Trunk)

Table 40: CO-DS1 (DS1 CO Trunk)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
CO-DS1	MAJOR**	test trunk *group# member#* l	DS1 CO Trunk
CO-DS1	MINOR	test trunk *group# member#* l	DS1 CO Trunk
CO-DS1	WARNING	test trunk *group# member#*	DS1 CO Trunk
Note: For Avaya G350 systems you must consult local records for the location and designation of the equipment rack where the G350 is mounted.			
A Major alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options command and that at least 75 percent of the trunks in this trunk group are alarmed.			

The MM710 supports T1/E1, and delivers the same functionality as the DEFINITY TN464 circuit pack.

Many trunk problems are caused by incorrect settings of parameters on the trunk group administration form. Settings must be compatible with the local environment and with parameter settings on the far-end. Refer to *"Chapter 12, Managing Trunks"* in the *Administrator's Guide for Avaya Communication Manager,* 555-233-506 for information on how to administer trunks. For the correct settings for administrable timers and other parameters on a country-by-country basis, see your local Avaya representative.

A DS1 CO (central office) trunk provides a link for digitized voice or data communications between the system and a central office switch. There are two types of DS1 interfaces:

- 24 DS0 channels on a 1.544 Mbps link
- 31 DS0 channels + 1 framing channel on a 2.048 Mbps link

  32-channel mode is supported on TN464 Media Modules and on MM710 Media Modules.

The CO-DS1 maintenance object monitors and maintains a CO trunk port on a MM710 Interface Media Module. See MG-DS1 in this chapter for more information about this Media Module. The DS1 Media Module supports low level CO trunk signaling interfaces for both ground-start and loop-start trunks. This maintenance strategy covers the in-line errors log, initialization tests, periodic tests, scheduled tests, demand tests, and alarm resolution.

Three trunk service states are specified by DS1 CO trunk maintenance:

Table 41: Trunk Service States

out-of-service	The trunk is in a deactivated state and cannot be used for either incoming or outgoing calls.
in-service	The trunk is in an activated state and can be used for both incoming and outgoing calls.
disconnect (ready-for-service)	The trunk is in an activated state but can only be used for an incoming call.

Error Log Entries and Test to Clear Values

Table 42: CO-DS1 Trunk Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test trunk <grp>/<mbr>
1(a)	57408				

1 of 2

Table 42: CO-DS1 Trunk Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
1(a)	57487				
15(b)	Any	Port Audit and Update Test (#36)			
18(c)	0	busyout trunk <grp>/<mbr>	WARNING	OFF	release trunk <grp>/ <mbr>
130(d)		None	WARNING	ON	test trunk <grp>/<mbr>
769(g)	57484				
1793(h)					test board GGGVSpp l
2562(i))	16665				
2817(j)	52992				
3840(k)		Port Audit and Update Test (#36)			
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					
**Major alarms MO may be downgraded to Warning alarms based on the value used in the set options command.					

2 of 2

Notes:

- (a) Error Type 1—Aux Data 57408—No tip ground is detected on an outgoing call. Aux Data 57487—PBX could not get “loop close” signal.
- (b) Error Type 15—This is a software audit error that does not indicate any hardware malfunction. Run Short Test Sequence and investigate associated errors (if any).
- (c) Error Type 18—System Technician has busied out the trunk to the out-of-service state. No calls can be made on this trunk except the Facility Access Test Call.
- (d) Error Type 130—This error type indicates that the Media Module has been removed or has been insane for more than 11-minutes. To clear the error, reinsert or replace the Media Module.
- (g) Error Type 769—The DS1 Interface Media Module detects a hardware fault. The Aux Data field contains the following error type:—57484, fault is detected on tip/ring.
- (h) Error Type 1793—DS1 Interface Media Module is out-of-service. Look for MG-DS1 errors in the Hardware Error Log. Refer to the DS1 Trunk Media Module or MG-DS1 Media Module Maintenance documentation for details.

- (i) Error Type 2562—Retry Failure error. This error is logged only. It is not a hardware failure and hence does not start any testing or generate any alarms. This error comes from call processing and is generated when a second attempt (retry) to seize an outgoing trunk fails.
- (j) Error Type 2817—Glare error. This error is logged only. It is not a hardware failure and hence does not start any testing or generate any alarms. This error is the result of a simultaneous seizure of a two-way trunk from both the near-end and the far-end. Attempt to place the call again. If the error persists, escalate.
- (k) Error Type 3840—Port Audit and Update Test (#36) failed due to an internal system error. Enter the **status trunk** command to verify the status of the trunk. If the trunk is out-of-service, then enter the **release trunk** command to put it back into in-service. Retry the test command.

System Technician-Demanded Tests: Descriptions and Error Codes

CAUTION:

Always investigate tests in the order they are presented in the table below when inspecting errors in the system. By clearing error codes associated with the NPE *Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 43: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** This Test ABORTS		X	ND
Conference Circuit Test (#7) **Note:** This Test ABORTS		X	ND
DS1 CO Trunk Seizure Test (#314) **Note:** This Test ABORTS	X	X	ND
Port Audit and Update Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Port Audit and Update Test (#36)

This test sends port level translation data from switch processor to the DS1 Interface Media Module to assure that the trunk's translation is correct. Translation updates include the following data: trunk type (in/out), dial type, timing parameters, and signaling bits enabled. The port audit operation verifies the consistency of the current state of trunk.

Table 44: TEST #36 Port Audit and Update Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals for a maximum of 5 times.
1000	ABORT	System resources required to run this test were not available. The port may be busy with a valid call. Use **display port GGGVSPP** to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. If the port status is active but the port is not in use (no calls), check the error log for error type 1025. The port may be locked up. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1006	ABORT	The DS1 CO trunk is out of service. Use **status trunk** to verify that the trunk is out of service. If the trunk is out of service, determine why. If it is OK to put the trunk back in service, use the **release trunk** command to put the trunk back in service, and then retry the test.
2000	ABORT	Response to the test was not received within the allowable time period.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	Test failed due to internal system error. Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 2

Table 44: TEST #36 Port Audit and Update Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	Trunk translation has been updated successfully. The current trunk states kept in the DS1 Interface Media Module and switch software are consistent. If the trunk is busied out, the test will not run but will return PASS. To verify that the trunk is in-service: Enter **status trunk** to verify that the trunk is in-service. If the trunk is in-service, no further action is necessary. If the trunk is out-of-service. Enter **release trunk** to put the trunk back into in-service. Retry the test command.
Any	NO BOARD	The test could not relate the internal ID to the port. This result could be due to incorrect translations, no board inserted, an incorrect board inserted, an insane board inserted, or the board is hyperactive. Check to ensure that the board translations are correct. Use the **list config** command, and resolve any problems that are found. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port. If not, to check that there is a valid board inserted. Hyperactivity causes some special problems with the sequence suggested above. If the ports are translated after issuing the **list config** command but the 'Vintage' field reports that there is no board (when there really is a board), then the **busyout board** and the **release busy board** commands do not work (even though the **reset board** command does work). The software puts the hyperactive board back in service after the hyperactivity clears.

2 of 2

CO-TRK (Analog CO Trunk)

Table 45: CO-TRK (Analog CO Trunk)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
CO-TRK	MAJOR**	test port GGGVSpp l	Analog CO Trunk
CO-TRK	MINOR	test port GGGVSpp l	Analog CO Trunk
CO-TRK	WARNING	test port GGGVSpp l	Analog CO Trunk
Note: For Avaya G350 systems you must consult local records for the location and designation of the equipment rack where the G350 is mounted.			
A MAJOR alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options command and that at least 75% of the trunks in this trunk group are alarmed.			

Analog CO trunks are 2-wire analog lines to the CO which support both incoming and outgoing calls. CO trunk Media Modules have eight ports.

Interactions Between Switch and CO

The following sequences show the interactions between the switch and the CO during call setup for both loop-start and ground-start trunks.

Loop Start Operation

Idle State:

Tip = ground, Ring = CO Battery

Outgoing Call:

1. PBX Off-Hook (Seize Message): Closes the Tip-Ring Loop.
2. CO Response: DC loop current + Dial tone.
3. PBX On-Hook (Drop Message): Open Tip-Ring loop, no loop current.
4. CO Response: CO goes to idle state (see Note).

Incoming Call:

1. CO Applies Ringing Voltage.
   a. PBX Response: Detect ringing current.
2. PBX Off-Hook (Answer Message): Close Loop.
   a. CO Response: Trip ringing, provide loop current.
3. PBX On-Hook (Drop Message): Open Tip-Ring Loop, no Loop Current.
   a. CO Response: CO goes to idle state (see Note).

Note:

CO does not normally provide an On-Hook (Disconnect) signal. Exceptions to this rule include Netherlands loop start and UK loop-calling guarded-clearing.

Ground Start Operation

Idle state:

Tip = open, Ring = CO Battery

Outgoing Call:

1. PBX Off-Hook (Seize Message): Places ground on Ring.
   a. CO Response: Places ground on Tip.
   b. PBX Response: Close the loop.
   c. CO Response: Provide loop current.
   d. PBX response: Dial out digits.
2. PBX On-Hook first (Drop Message): Open the Tip-Ring Loop, no loop current.
   a. CO Response: Open circuit on Tip.
3. CO On-Hook first (Disconnect): Open circuit on Tip, no loop current.
   a. PBX Response: Open Tip-Ring loop.

Incoming Call:

1. CO Off-Hook (Seizure): CO applies ground on Tip and applies ringing voltage.
   a. PBX Response: Make trunk busy for outgoing calls.
2. CO Ringing: CO applies ringing voltage.
   a. PBX Response: Detect ringing, ring destination.
3. PBX Off-Hook (Answer Message): Close loop.
   a. CO Response: Trip ringing, provide loop current.

4. PBX On-Hook first (Drop Message): Open the Tip-Ring Loop, no loop current.
   a. CO Response: Open circuit on Tip.
5. CO On-Hook first (Disconnect): Open circuit on Tip, no loop current.

Error Log Entries and Test to Clear Values

Table 46: CO Trunk Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port *GGGVSpp* sh r 1
1 (a)	57347	None			
15 (b)	any	Port Audit Update Test (#36)			
18	0	busyout trunk	WARNING	OFF	release trunk *grp#/mbr#*
130(c)		None	WARNING	ON	test port *GGGVSpp* sh r 2
257 (a)	50176	None			
513 (a)	57364	None	MAJ/MIN/WRN**	ON	
769 (a)	57392	None	MAJ/MIN/WRN**	OFF	
1025 (e)	Any	Demand Diagnostic Test (#3)	MAJ/MIN/WRN**	OFF	test port *GGGVSpp* sh r 2
1281 (e)	Any	Demand Diagnostic Test (#3)	MAJ/MIN/WRN**	ON	test port *GGGVSpp* sh r 3
1537		Dial Tone Test (#0)	MAJ/MIN/WRN**	OFF	test port *GGGVSpp* l r 2
2561 (d)	57345	None			
2817 (a)	57360	None			
2817 (a)	57393	None			

1 of 2

Table 46: CO Trunk Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
2817 (d)	57484	Dial Tone Test(#0)	MAJ/MIN/ WRN	OFF	test port *GGGVSpp* l r 1
3073 (d)	57376	None			
3329 (d)	57408	None			
3329 (d)	57484	Dial Tone Test(#0)	MAJ/MIN/ WRN	OFF	test port *GGGVSpp* l r 1
3585 (d)	57424	None			
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					
**Major alarms may be downgraded to Warning alarms based on the value used in the set options command.					
2 of 2					

Notes:

- (a) In-line errors that have no specific test associated with them. Refer to the following table for an explanation and appropriate action.
- (b) A software audit error that does not indicate any hardware malfunction. Run Short Test Sequence and investigate associated errors.
- (c) Indicates that the Media Module has been removed or has been insane for at least 11-minutes. To clear the error, reinsert or replace the Media Module.
- (d) Aux data 57345 - Single polarity ringing current

  Aux data 57376 - No loop current on incoming call

  Aux data 57408 - No tip ground detected on outgoing call

  Aux data 57424 - No loop current on outgoing call

  Aux data 57484 - No dial tone on outgoing call

  These errors cause the Dial Tone Test (#0) to run and are only considered a problem if the Dial Tone Test fails (in which case Error Type 1537 will also show up). In this case, the trunk may be put in Ready-For-Service state (shown as disconnected by status command), which allows only incoming calls. Run the Dial Tone Test (#0) and follow its outlined procedures.

  If error count associated with this error type is very high (i.e., 225) and if Alarm Status on the Hardware Error Report is n (not alarmed), then the existence of this error type indicates that, despite the fact that many in-line error messages have been received, all Call Seizure Tests have passed. Problems at the CO may cause this condition rather than problems with the PBX.

- If test fails after two repetitions, replace Media Module.

  Check for the use of MFT/Range extenders. If there are extenders present, and there are no other complaints or maintenance errors against this trunk, then there is a good chance that Test #3 failed due to excessive loop current and may be ignored.

Table 47: CO Trunk Errors with No Tests *1 of 3*

Error Type	Aux Data	Error Description and Repair Action
1	57347	Port error. Ringing without ground. This error is detected on an incoming call on a ground-start CO trunk. The CO trunk Media Module has not detected a Tip ground before ringing current is detected. This may indicate that the ground detector is not working. However, the call will be accepted. Busyout the affected port, and run a long test. Observe the test results. If any tests fail, refer to the description of the tests and the associated error codes. Release the port. If users continue to report troubles, check for other errors and make test calls to determine whether the problem should be referred to the CO.
257	50176	Battery reversal detected. This is usually caused by the CO (often seen with step-by-step and cross-bar offices in connection with outgoing calls). This is detected if the direction of the loop current changes from normal to reverse for at least 40 msec. Could occur if the trunk was just installed and for some reason the Tip and Ring wires were reversed at the PBX. If battery reversals occur during dialing, wrong numbers may result. Refer problem to CO. Ask them to remove the battery reversal option.
513	57364	Ground detector stuck active. After several occurrences, an on-board minor alarm is generated. Run the short test sequence. If test aborts with Error Code 1000, disconnect Tip and Ring and repeat short test. If test still aborts, replace Media Module. If test passes, refer problem to CO. If any other error code is received, pursue that problem.
769	57392	CO not releasing after call is dropped from PBX end, or the loop is not open after a disconnect. After several occurrences, an off-board warning alarm is generated. Refer problem to CO.

1 of 3

Table 47: CO Trunk Errors with No Tests *2 of 3*

Error Type	Aux Data	Error Description and Repair Action
2561	57345	Single polarity ringing current. This error results from abnormal ringing current, but does not prevent the incoming call from being accepted. One cause could be that the reverse current detector associated with the port is failing. (Will not be detected by any tests.) Another cause could be that normal current is not detected. In this case, neither incoming nor outgoing calls can be completed, and the dial tone test will also fail. The last cause could be that certain types of noise are present on the CO line during the silent period of ringing. First check for other errors. If the count for this error is very high (255), and all tests pass, then either the reverse current detector is defective or the CO line is noisy. If the CO line is suspect, make Tip and Ring observations. If the line is determined to be noisy, refer the problem to the CO. If the reverse current detector is defective, ignore this error.
2817	57360	Ground but no ringing. This error occurs on an incoming call on a ground-start trunk. If ringing is not detected within 5 seconds of the Tip being grounded, the call is still accepted. If the CO is of the No. 5ESS. switch type, ringing delays of more than 5 seconds during heavy traffic are fairly common. Check for other errors.
2817	57393	The loop is opening too slowly after a disconnect. This error indicates an on-board problem, although the trunk may be functional. Check for other errors.
3073	57376	No loop current on incoming call. The incoming destination has already answered and no loop current has been detected. If this is a hard fault, the dial tone test and all outgoing calls should also fail. Check for other errors.

2 of 3

Table 47: CO Trunk Errors with No Tests *3 of 3*

Error Type	Aux Data	Error Description and Repair Action
3329	57408	Trunk error. No Tip ground detected on outgoing call. This error occurs when an attempt is made to seize a ground-start CO trunk for an outgoing call and Tip ground is not detected or the caller hangs up before Tip ground is detected. Busyout the affected port, and run a long test. Observe the test results. If any tests fail, refer to the description of the tests and the associated error codes. Release the port. If users continue to report troubles, check for other errors and make test calls to determine whether the problem should be referred to the CO. Busyout the affected port, and run a long test. If Dial Tone Test #0 passes, ignore this error. Release the port.
3585	57424	No loop current on outgoing call. This error occurs on attempt to seize a loop or ground-start trunk for an outgoing call. An error occurs if loop current is not detected or the caller hangs up before it is detected. Busyout the affected port, and run a long test. If CO Demand Diagnostic Test #3 passes and this error keeps occurring, refer problems to CO. Release the port.
		3 of 3

System Technician-Demanded Tests: Descriptions and Error Codes

Always investigate tests in the order they are presented in the table below when inspecting errors in the system. By clearing error codes associated with the NPE *Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 48: Order of Investigation *1 of 2*

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** *This Test will abort with Error Code 1412*		X	ND
Dial Tone Test (#0)		X	ND
			1 of 2

Table 48: Order of Investigation *2 of 2*

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
CO Demand Diagnostic Test (#3)	X	X	ND
Looparound and Conference Test (#33) **Note:** *This Test will abort with Error Code 1412.*		X	ND
Audit Update Test (#36)	X	X	ND
Transmission Test - ATMS (#844-848) **Note:** *This Test will abort with Error Code 1412*			ND
*D = Destructive; ND = Nondestructive			
			2 of 2

If errors logged by test #3 are the only complaints against this trunk, then the system technician should check if MFT/Range Extenders are being used. If extenders are present, then there is a good chance that there is excessive loop current, which will cause Test #3 to log errors.

However, all else being normal, these errors should not affect the customer.

Dial Tone Test (#0)

This test attempts to seize a port and checks for the return of a dial tone.

Table 49: Test #0 Dial Tone Test *1 of 4*

Error Code	Test Result	Description/ Recommendation
	ABORT	Could not allocate system resources to run this test. 1. Retry the command at 1-minute intervals for a maximum of 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. 1. Use the command **display port UUCSSpp** to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the service state indicates that the port is in use, then the port is unavailable for certain tests. You must wait until the port is idle before retesting. 2. Retry the command at 1-minute intervals for a maximum of 5 times.
1001	ABORT	System resources required to run this test were not available. This could be due to a failure to seize the port. 1. Retry the command at 1-minute intervals for a maximum of 5 times.
1002	ABORT	The system could not allocate time slots for the test. The system may be under heavy traffic conditions or it may have time slots out-of-service due to TDM-BUS errors. 1. If the system has no TDM-BUS errors and is not handling heavy traffic, retry the command at 1-minute intervals for a maximum of 5 times.

1 of 4

Table 49: Test #0 Dial Tone Test *2 of 4*

Error Code	Test Result	Description/ Recommendation
1004	ABORT	The port was seized by a user for a valid call. 1. Use the **display port UUCSSpp** command to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the service state indicates that the port is in use, then the port is unavailable for certain tests. You must wait until the port is idle before retesting. 2. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1005	ABORT	Trunk has been administered as incoming-only; dial tone can only be obtained on outgoing trunks. This is a normal condition.
1018	ABORT	Test has been disabled via administration. 1. Verify that the “Maintenance Tests?” field on the Trunk Group Form is set to “n.” To enable the test, use the **change trunk-group x** command where “x” equals the number of the trunk group to be tested. Then change the entry in the “Maintenance Tests?” field on the form to “y.”
2000	ABORT	Response to the test was not received within the allowable time period. 1. Retry the command at 1-minute intervals for a maximum of 5 times.

2 of 4

Table 49: Test #0 Dial Tone Test *3 of 4*

Error Code	Test Result	Description/ Recommendation
	FAIL	Trunk was seized, but dial tone could not be detected. 1. Test all administered outgoing ports on the board. Failure of 1 indicates a problem toward the CO. 2. If all fail, see note below. 3. Check for errors on the TONE-BD or TONE-PT. Clear any errors found, and repeat the test. 4. If the error has still not cleared, refer the problem to the CO. 5. If no service problems exist on the port, continue to use the port until the circuit pack can be replaced (as a last resort). Perform a trunk test call to see if the trunk is operable. **Note:** If the dial tone test fails for all ports on a circuit pack, a -5 volt power problem is indicated. To investigate problems with a power unit, refer to “CARR-POW”.
2002	FAIL	Seizure portion of test failed due to hardware problem. Fault is usually caused by a disconnected trunk. 1. If the CO Demand Diagnostic Test (#3) also failed, display the Hardware Error Log. If the CO Demand Diagnostic Test failed because it could not detect ground (indicated by Error Type 1281 in the Hardware Error Log) AND Error Type 3329 or 3585 appears in the Hardware Error Log (with the same last occurred time as Error Type 1281 and 1537), replace the circuit pack. 2. Check trunk wiring to ensure good connection; repeat test if wiring correction made. 3. Locate another identical CO trunk and swap its wiring with one under test. Repeat test on both trunks and determine if problem follows trunk or remains at original port. If problem follows trunk, refer problem to CO. If problem remains at port, replace circuit pack and repeat test.
1009	PASS	Detected tone was not pure dial tone. No action required.

3 of 4

Table 49: Test #0 Dial Tone Test *4 of 4*

Error Code	Test Result	Description/ Recommendation
	PASS	Trunk was seized, and dial tone was detected. User-reported troubles on this port should be investigated by using other port tests and by examining trunk or external wiring.
0	NO BOARD	The test could not relate the internal ID to the port. 1. Check to ensure that the board translations are correct. Translate the board, if necessary. 2. Use the **busyout board** command. 3. Use the **reset board** command. 4. Use the **release busy board** command. 5. Use the **test board** command. This should re-establish the linkage between the internal ID and the port.

4 of 4

CO Demand Diagnostic Test (#3)

For ground start trunks, port Media Module relays are operated and checks are made to see if the port can detect and apply ground on the Tip lead. This test also verifies that there is no external ground on the Ring lead. In the absence of other failures, the Media Module should be replaced only if this test fails with the CO line disconnected.

This test also checks the on-board programmable transmission circuits that allow the Media Module to support transmission characteristics of several different countries.

Table 50: TEST #3 CO Demand Diagnostic Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Could not allocate system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. Use the **display port GGGVSpp** command to determine the trunk group/ member number of the port. Use the **status trunk** command to determine the service state of the port. If the service state indicates that the port is in use, then the port is unavailable for certain tests. You must wait until the port is idle before retesting. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1004	ABORT	The port was seized by a user for a valid call. Use the **display port GGGVSpp** command to determine the trunk group/ member number of the port. Use the **status trunk** command to determine the service state of the port. If the service state indicates that the port is in use, then the port is unavailable for certain tests. You must wait until the port is idle before retesting. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1005	ABORT	Test inapplicable to present configuration. This is a normal condition.
1018	ABORT	Test has been disabled via administration. For this test to run, the `Maintenance Tests?` field on the trunk group form must be set to `n`. The form is accessed with the change trunk-group grp# command.
2000	ABORT	Response to the test was not received within the allowable time period. Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 2

Table 50: TEST #3 CO Demand Diagnostic Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	FAIL	Failure to detect ground or faulty ground detected on Ring lead. Display the hardware errors for this trunk, to determine if the fault was on- or-off board. Look for Error Type 1025 or 1281 (if both appear in the Hardware Error Log, pick the most recent error). Error Type 1025 indicates a faulty ground detected on Ring lead (an off-board fault) and Error Type 1281 indicates failure to detect (internally generated) ground (an on-board fault). Faulty ground detected on Ring lead (Error Type 1025): Repeat test. If test passes, ignore the original failure. If test aborts, follow the recommended procedures. Repeat test with CO line removed. If test fails, replace the Media Module. If test passes, refer problem to CO. Failure to detect ground (Error Type 1281): Run the long test sequence. If the CO Demand Diagnostic Test fails, the Dial Tone Test (#0) fails with Error Code 2002, AND Error Type 3329 or 3585 appears in the Hardware Error Log (with the same last occurred time as Error Type 1281 and 1537), replace the Media Module. Repeat test with CO line removed. If test fails, replace the Media Module. If test passes, the CO may be drawing too much current. Refer problem to CO.
	PASS	This test verifies that the port is able to apply ground for outgoing calls and detect ground for incoming calls; however, it does not provide information on whether a CO line is actually connected. User-reported troubles on this port should be investigated by using other port tests and by examining trunk or external wiring.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

Port Audit Update Test (#36)

This test will send updates of the CO port translation for all ports on the Media Module which have been translated. The update is non-disruptive and guards against possible corruption of translation data contained on the Media Module. No response message is expected from the Media Module once it receives translation updates. The port translation data includes: ground or loop start trunk, tone or rotary dialing trunk, rotary dialing inter-digit timing, network balance R/RC, and disconnect timing.

Table 51: TEST #36 Port Audit Update Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1006	ABORT	The port has been placed out of service, perhaps by craft busyout. Use the **display port GGGVSpp** command to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the service state indicates that the port is in use, wait until the port is idle before testing. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
2100	ABORT	System resources required to run this test were not available. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	Internal system error Retry the command at 1-minute intervals for a maximum of 5 times.
	PASS	This test passed. Translation information was successfully updated on the Media Module. User-reported troubles on this port should be investigated by using other port tests and by examining trunk or external wiring. If the trunk is busied out, the test will not run, but will return PASS. To verify that the trunk is in-service: Enter **status trunk** to verify that the trunk is in-service. If the trunk is in-service, no further action is necessary. If the trunk is out-of-service, continue to Step 2. Enter **release trunk** command to put trunk back into in-service. Retry the test command.

1 of 2

Table 51: TEST #36 Port Audit Update Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
Any	NO BOARD	The test could not relate the internal ID to the port (no board). Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

DID-DS1 (Direct Inward Dial Trunk)

Table 52: DID-DS1 (Direct Inward Dial Trunk)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run	Full Name of MO
DID-DS1	MAJOR*	test trunk *grp*/*mbr* l	Direct Inward Dial Trunk
DID-DS1	MINOR	test trunk *grp*/*mbr* l	Direct Inward Dial Trunk
DID-DS1	WARNING	test trunk *grp*/*mbr*	Direct Inward Dial Trunk
*A Major alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options** command and that at least 75 percent of the trunks in this trunk group are alarmed. For more information on the **set options** command			

The DID-DS1 trunk provides a digital Direct Inward Dial (DID) trunk from a CO switch to the system through a DS1 link. A 24-channel DS1 link can support up to 24 DID-DS1 trunk calls simultaneously. A 32-channel link can support up to 30. A DID-DS1 trunk can be used for digitized voice and data communications with appropriate DS1 signaling mode (for example, common channel signaling). The MM710 series Media Modules support wink-start and immediate-start trunks and call processing signaling. See MG-DS1 for more information. Throughout this section, the term DS1 applies to MM710 Media Modules.

Information included in this section covers the in-line errors log, initialization tests, periodic tests, scheduled tests, system technician demand tests, and alarms escalation and elimination. Two trunk service states are specified in the DID-DS1 trunk maintenance:

- `out-of-service` – The trunk is in a deactivated state and cannot be used for incoming calls.
- `in-service` – The trunk is in an activated state and can be used for incoming calls.

If the DS1 Media Module is out-of-service, then all trunks on the DS1 Interface Media Module are put into the out-of-service state and a Warning alarm is raised.

Error Log Entries and Test to Clear Values

Table 53: DID-DS1 Trunk Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test trunk *grp#/mbr#*
1(a)	Any				
15(b)	Any	Port Audit and Update Test (#36)			
18(c)			WARNING	OFF	release trunk *grp#/mbr#*
130(d)		None	WARNING	ON	test trunk *grp#/mbr#*
257(e)	57474 57473				
513(f)	57392		MIN/MAJ**		
769(g)	57393		MIN/MAJ**		
1793(h)					test board *GGGVSpp*
2305(i)	50944	None	MIN/MAJ**	OFF	
3840(j)		Port Audit and Update Test (#36)			

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

1 of 2

Table 53: DID-DS1 Trunk Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
**This alarm will only be raised when the System-Parameter Country form has the Base Tone Generator field set to 4 (Italy). This alarm will be a MINOR alarm unless 75% or more trunks in this trunk group are out of service, then the alarm will be upgraded to a MAJOR alarm.					
***Major alarms may be downgraded to Warning alarms based on the value used in the set options command.					
					2 of 2

Notes:

- (a) Error Type 1—DS1 Interface Media Module detects a hardware error on the DS1 DID trunk. The Aux Data field indicates the following:

57476	On-hook before wink
57477	On-hook before ready to receive digits
57485	Wink too short for valid signal

Maintenance does not start any testing or generate any alarms in response to these errors.

- (b) Error Type 15—This is a software audit error that does not indicate any hardware malfunction. Run Short Test Sequence and investigate errors (if any).
- (c) Error Type 18—The trunk has been taken out of service by a demand busyout. No calls can be made on this trunk.
- (d) Error Type 130—This error type indicates that the Media Module has been removed or has been insane for more than 11 minutes. To clear the error, reinsert or replace the Media Module.
- (e) Error Type 257—DS1 Interface Media Module detects a hardware error on the DS1 DID trunk. The Aux Data field indicate the source of the error:

57474	Rotary dial rate above 12 pulses per second
57473	Rotary dial rate below 8 pulses per second

- (f) Error Type 513—DS1 Interface Media Module detects a hardware error on the DS1 DID trunk. Aux Data 57392 indicates no external release on PBX disconnect.
- (g) Error Type 769—DS1 Interface Media Module detects a hardware error on the DS1 DID trunk. Aux Data 57393 indicates belated external release on PBX disconnect.
- (h) Error Type 1793—DS1 Interface Media Module is out-of-service. Look for MG-DS1 errors in Hardware Error Log. Refer to the appropriate “MG-DS1” information for details.

- (i) Error Type 2305—This error indicates that a signaling change was detected by the PBX trunk Media Module which is inconsistent with the present state of the trunk.
- (j) Error Type 3840—Port Audit and Update Test (#36) failed due to an internal system error. Enter **status trunk** command to verify the status of the trunk. If the trunk is out-of-service, then enter the **release trunk** command to put it back to in-service. Retry the test command.

System Technician-Demanded Tests: Descriptions and Error Codes

CAUTION:

Always investigate tests in the order they are presented in the table below. By clearing error codes associated with the NPE *Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 54: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** *This test will abort with Error Code 1412*		X	ND
Conference Circuit Test (#7) **Note:** *This test will abort with Error Code 1412*		X	ND
Port Audit and Update Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Port Audit and Update Test (#36)

This test sends port level translation data from the switch processor to the DS1 Interface Media Module to assure that the trunk's translation is correct. The port audit operation verifies the consistency of the current state of the trunk as kept in the DS1 Interface Media Module and in the switch software.

Table 55: TEST #36 Port Audit and Update Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
1000	ABORT	The port may be busy with a valid call. Use **display port GGGVSpp** to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. If the port status is active but the port is not in use (no calls), check the error log for error type 1025. The port may be locked up. If the port status is idle, retry the command at 1-minute intervals a maximum of 5 times.
1006	ABORT	The test was aborted because the trunk is out of service. Use **status trunk** to verify that the trunk is out of service. If the trunk is out of service, determine why. To put the trunk back in service, use the **release trunk** command. Retry the test.
2000	ABORT	Response to the test was not received in the allowable time period.
2100	ABORT	Could not allocate resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Test failed due to internal system error. Retry the command at 1-minute intervals a maximum of 5 times.

1 of 2

Table 55: TEST #36 Port Audit and Update Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	Trunk translation has been updated successfully. The current trunk states kept in the DS1 Interface Media Module and switch software are consistent. If the trunk is busied out, the test will not run but will return PASS. To verify that the trunk is in-service: Enter **status trunk** to verify that the trunk is in-service. If the trunk is in-service, no further action is necessary. If the trunk is out-of-service. Enter **release trunk** to put the trunk back into in-service. Retry the test command.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Check to ensure that the board translations are correct. Use the **list config** command, and resolve any problems that are found. If the board was found to be correctly inserted in step 1, use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port. If this is not the case, check to see that there is a valid board inserted.

2 of 2

DID-TRK (Direct Inward Dial Trunk)

Table 56: DID-TRK (Direct Inward Dial Trunk)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
DID-TRK	MAJOR**	test port GGGVSpp l	DID Trunk
DID-TRK	MINOR	test port GGGVSpp l	DID Trunk
DID-TRK	WARNING	None	DID Trunk
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			
A MAJOR alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options command and that at least 75 percent of the trunks in this trunk group are alarmed.			

Many trunk problems are caused by incorrect settings of parameters on the trunk group administration form. Settings must be compatible with the local environment and with parameter settings on the far-end. Refer to *Administrator's Guide for Avaya Communication Manager, 555-233-506*, for information on how to administer trunks. For the correct settings for administrable timers and other parameters on a country-by-country basis, see your local Avaya representative.

Direct Inward Dial trunks connect the switch to the CO, and allow outside parties to call directly to an extension in the system. MM711 supports eight incoming-only ports.

DID Trunk Operation

The DID port receives three to five digits from the CO that are used to directly connect an outside caller to the called station without assistance from an attendant. For each call, the CO switch signals the system by opening and closing individual DID loops (one of the eight ports), causing the starting or stopping of loop current.

DID Trunk Testing

The system uses technician-invoked tests to diagnose the health of the trunk. These tests are described in the following sections. Additionally, in-line testing, which can generate errors, is performed while a call is in progress. See the Error Log Table 57: DID Trunk Error Log Entries on page 126 for a description of these errors. These errors may be reproduced by placing a call on the trunk and checking the Hardware Error Log.

Problems detected during signaling may be caused by off-board faults in the CO switch or connections for which a Warning alarm is raised.

Before a maintenance test can be run on a port, the port must be idle. If an incoming call seizes a port that is being tested, the test will abort and the incoming call will proceed.

For transmission and signaling standard specification, refer to *Digital PBX Standards*, RS4648.

Ports Out-of-Service without Errors or Alarms

A common trouble on DID trunks that produces no errors or alarms occurs when the CO busies out (disconnects) the port. This situation occurs when the CO thinks there are problems with the DID port. In this case, no incoming calls will be possible through this port. This may result in complaints from outside callers trying unsuccessfully to call in. This problem can be diagnosed by listing measurements on lightly used trunks. If a particular port is detected as not in use, a call to the CO will be necessary to get the connection back in service.

Error Log Entries and Test to Clear Values

Table 57: DID Trunk Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port *GGGVSpp* sh r 1
1(a)	Any	None	WRN	OFF	
1(b)	57476	None	WRN	OFF	
1(c)	57477	None	WRN	OFF	
1(d)	57483	None	WRN	OFF	

1 of 2

Table 57: DID Trunk Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
15(e)	Any	Port Audit Update (#36)			
18	0	busyout trunk *grp/mbr*	WRN	OFF	release trunk *grp/mbr*
130(f)		None	WRN	ON	test trunk *grp/mbr*
257(g)	57472	None	WRN	OFF	
257(h)	57473	None	WRN	OFF	
257(i)	57474	None	WRN	OFF	
257(j)	57475	None	WRN	OFF	
513(k)	57392	None	MIN/ WRN**	OFF	
513(l)	57393	None			
769	Any	Port Diagnostic (#35)	MIN/ WRN**	ON	test port *GGGVSpp* r 3
1537	Any	Port Diagnostic (#35)	MAJ/ MIN/ WRN**	OFF	test port *GGGVSpp* r 3

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

**Major alarms may be downgraded to Warning alarms based on the value used in the set options command.

2 of 2

Notes:

See also the preceding section on trunk problems without errors or alarms.

- (a) This condition occurs when the tone detector times out waiting for digits. Change wink/ immediate-start parameter to wink/immediate-start and rotary/tone-dial parameters.

  1. Verify trunk administered wink/immediate-start parameter.
  2. Test trunk using BUTT set.
  3. Refer problem to CO.

- (b) Rotary dial before wink — This condition occurs when the CO starts dialing before the PBX sends wink on a wink-start trunk.
  1. Verify trunk administered wink/immediate-start parameter.
  2. Refer problem to CO.
- (c) Rotary dial too early — This condition occurs when the CO starts dialing too soon after seizure on an immediate-start trunk.
  1. Verify trunk administered wink/immediate-start parameter.
  2. Refer problem to CO.
- (d) Rotary dial pulse during wink — This condition occurs when the CO sends rotary dial digits too soon after seizure on a wink-start trunk.
  1. Verify trunk administered wink/immediate-start parameter.
  2. Refer problem to CO.
- (e) This is a software audit error that does not indicate any hardware malfunction. Run Short Test Sequence and investigate associated errors (if any).
- (f) This error type indicates that the Media Module has been removed or has been insane for more than 11 minutes. To clear the error, reinsert or replace the Media Module.
- (g) Rotary dial pulse on-hook longer than 105 msec — Break between rotary pulses is too long.
  1. Test trunk by performing an incoming test call.
  2. Refer problem to CO.
- (h) Rotary dial rate below 8 pulses/sec — More than 135 msec between two successive breaks.
  1. Verify trunk administered interdigit-timing parameters.
  2. Refer problem to CO.
- (i) Rotary dial rate above 12 pulses/sec — Less than 75 msec between two successive breaks.
  1. Verify trunk administered interdigit-timing parameters.
  2. Refer problem to CO.
- (j) Digit detection — CO is starting new rotary dial digit within 150 msec of previous digit.
  1. Verify trunk administered interdigit timing parameters.
  2. Refer problem to CO.

- (k) Loop current active — CO not releasing trunk after PBX disconnect. Occurs when the PBX end drops first and the CO does not release the trunk within 4 minutes.

  1. Verify the interface to the network with a hand telephone set. If calls are placed correctly, then refer problem to the CO.
  2. If unable to place calls or this equipment is not available, check the status on port using the **status trunk** command. If active but not connected, disconnect bridging clips at the network interface. Check status on the trunk. If trunk went idle, then replace clips. If trunk is still active but unable to place calls, refer problem to the CO.

- (l) Late CO trunk release — This event only occurs after the occurrence of Error Type 513. The CO released the trunk 4 minutes after the PBX dropped the call. This event decrements the severity (error count) of Error Type 513, or may mean the problem related to Error Type 513 has been fixed.

  1. Verify that Error Type 513 does not occur again. Refer to Error 513.

System Technician-Demanded Tests: Descriptions and Error Codes

CAUTION:

Always investigate tests in the order presented in the table below. By clearing error codes associated with the NPE *Crosstalk Test* for example, you may also clear errors generated from subsequent tests in the testing sequence.

Table 58: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** *This test will abort with Error Code 1412*		X	ND
Port Diagnostic Test (#35)	X	X	ND
Looparound and Conference Circuit Test (#33) **Note:** *This test will abort with Error Code 1412*		X	ND
Port Audit Update Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Port Diagnostic Test (#35)

This test checks a port's battery feed circuitry for on-/off-hook detection, battery shutdown, and battery reversal (wink) capabilities.

Table 59: TEST #35 Port Diagnostic Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	System resources required to run this test were not available. Retry the command at 1-minute intervals a maximum of 5 times.
1000	ABORT	System resources required to run this test were not available. The port may be busy with a valid call. Enter **display port GGGVSpp** command to determine the trunk group/ member number of the port. Use the **status trunk** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. If the port status is active but the port is not in use (no calls), check the error log for Error Type 513. The port may be locked up. If the port status is idle, busyout and release the trunk, and retry the command at 1-minute intervals a maximum of 5 times. If the test continues to abort, check for wiring errors toward the CO which may cause the trunk to lock up. If the wiring is good and the test continues to abort, replace the circuit pack.
1004	ABORT	The port was seized by a valid call during the test. Enter **display port GGGVSpp** to determine the station extension, attendant number, or trunk group/member number of the port. Use the **status station**, **status attendant**, or **status trunk** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. Attendants are always in use (off-hook) if the handset is plugged in and the port is not busied out. Retry the command at 1-minute intervals a maximum of 5 times.
1018	ABORT	Test disabled via administration. Verify that the `Maintenance Tests?` field on the Trunk Group Form is set to n. To enable the test, use the **change trunk-group x** command (x is the trunk group number). Then change the entry in the `Maintenance Tests?` field to **y**.
2000	ABORT	Response to the test was not received within the allowable time period.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.

1 of 2

Table 59: TEST #35 Port Diagnostic Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
61446	FAIL	Battery feed test failed. A loop current fault was detected. This is most probably an incoming CO-line problem. This failure code is only reported by the TN2139 Italian DID Media Module. Check the incoming CO-line for loop current. If none is detected refer the problem to the CO. If the CO-line checks out OK, the failure must be on the DID port. Replace the Media Module.
61456	FAIL	Battery feed test failed. An on-board problem was detected. This port is out-of-service. Replace Media Module.
61472	FAIL	Battery feed test failed. A problem with the incoming CO-line was detected. Check the incoming CO-line for proper operation. If warranted, refer the problem to the CO. If the CO-line is not at fault, the failure must be on the DID port. Replace the Media Module.
	PASS	Current flow was detected for this port. User-reported troubles on this port should be investigated using other port tests and by examining connections. Refer problem to the CO.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port. If the problem persists, replace the circuit pack.

2 of 2

Port Audit Update Test (#36)

This test sends updates of the DID port translation for all ports on the Media Module that have been translated. The update is non-disruptive and guards against possible corruption of translation data contained on the Media Module. No response message is expected from the Media Module once it receives translation updates. The port translation data includes:

- Wink or immediate start trunk
- Dial tone or rotary dialing trunk
- Rotary dialing inter-digit timing
- Network balance R/RC
- Disconnect timing

Table 60: TEST #36 Port Audit Update Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.
1006	ABORT	The port is out of service, perhaps busied out. Use **display port GGGVSpp** to determine the trunk group/member number of the port. Use **status trunk** to determine the service state of the port. If the port is out of service, wait until the port is in service and idle before testing. If the port status is in service and idle, then retry the command at 1-minute intervals a maximum of 5 times.
2100	ABORT	Could not allocate the necessary system resources to run the test. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.

1 of 2

Table 60: TEST #36 Port Audit Update Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	This test passed. Translation information was successfully updated on the Media Module. If signaling troubles are reported (Error Types 1, 257, or 513), verify translation for this port. Refer problem to the CO.
Any	NO BOARD	The test could not relate the internal ID to the port. Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port. If the problem persists, replace the circuit pack.

2 of 2

DIG-LINE (Digital Line)

Table 61: DIG-LINE (Digital Line)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
DIG-LINE	MINOR	test port *GGGVSpp l*	Digital Line
DIG-LINE	WARNING	test port *GGGVSpp* sh	Digital Line

Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.

DIG-LINE maintenance monitors and tests ports on digital line Media Modules and the hardware connected to those ports for lines administered as a digital station. These include stations with just a digital voice terminal and stations with a digital voice terminal and a linked data module. Media Gateway-level maintenance is covered by “MG-DCP” whose strategy is described in the “XXX-BD (Common Port Media Module)” section.

Digital line maintenance interacts with digital line Media Module (MG-DCP) maintenance, and results of DIG-LINE testing can be affected by the health of the digital line Media Module. Keep this in mind when investigating digital line problems. There are instances where the service state of a station is mentioned. It is helpful to understand what is meant by the different service states that may exist. The different service states which apply to digital line station are explained as follows:

Out-of-Service	The port, and thus the station, have been removed from service. Busyout puts the port in the out-of-service state.
Ready-for-Service	The port on the Media Module has been put into service, but the voice terminal has not yet established signaling communications with the port.
In-Service	The voice terminal has established signaling communications with the port, and the system is ready to process calls to and from that station. A terminal in the ready-for-service state will progress to the in-service state if it is functioning normally. It can also be forced into the in-service state by going off-hook.

Programmable Terminals

The following information is presented to help you understand how maintenance software interacts with terminal parameter downloading.

Note:

MM711 supports 8410D and 8434D terminals
MM711 (2-wire, 8-port, A-law/mu-law selectable)

Downloadable Terminal Parameters

The following parameters are downloaded to programmable terminals:

Table 62: Parameters Downloadable to Programmable Terminals

Parameter	Scope	Terminal
International Flags (A-law/mu-law, Display Mode, DLI Voltage level)	System level	84xx, 603x, 302B1
Primary Levels (Transmission & Sidetone)	System level	84xx, 603x, 302B1
Adjunct Levels (Transmission & Sidetone)	System level	84xx
Handset Expander Option	System level	84xx
Administrable Options (Speakerphone & Mute Button)	Per-terminal	84xx
Administrable Softkeys	Per-terminal, System level	8410D, 8434D

Nonvolatile Memory

Nonvolatile memory stores downloadable parameters in programmable terminals. Once the terminal is downloaded, it is not be necessary to download it again, even if power is removed from the terminal. If nonvolatile memory fails with power still present, the terminal reverts to its default factory settings except for its A-law/mu-law companding settings which are stored in RAM. If power is removed after the nonvolatile memory fails, the terminal reverts to its factory default settings.

Note:

The mu-law companding mode is assigned as a default setting at the factory. For the United States, a programmable terminal can place calls even though it has not been downloaded from the system.

Download Actions

There are several different scenarios that cause a terminal to be downloaded. These can occur as part of background maintenance activity or on demand from the System Access Terminal or from a station.

For the background actions described below, the terminal downloads automatically if a download retry flag for the terminal is set in software. This flag is set at the time translation is loaded at boot time, when translation which affects the parameters of a terminal is changed as part of system administration actions, and when a port is inserted in software as a result of board insertion or translation change.

Automatic Download Actions

System Reboot/Restart

A global download action is started when periodic maintenance tests start after a system reboot/ restart regardless of whether the parameters have been downloaded previously.

Periodic Tests

If the download flag is still set when periodic tests are run on a terminal, a download action will occur. This operation is required in case a terminal could not be downloaded previously because it was off-hook at the time the system first booted or because the terminal was off-hook at the time translation associated with downloadable parameters was changed.

Note that it may take more than an hour for periodic tests to reach the terminal that needs to be downloaded.

Terminal Administration

A downloadable terminal is automatically downloaded when translation changes associated with downloadable parameters are made as part of system administration. As shown in the previous Table 62: Parameters Downloadable to Programmable Terminals on page 135, these changes can be for a specified terminal or may be system-wide. If the change is for system-level parameter, a background global update request is made to download all programmable terminals.

This global update may take more than an hour for a system with several thousand programmable terminals.

Port Insertion

Whenever maintenance software initiates a request to place a port into service, a terminal download action is started on that terminal if that terminal is programmable. This port insertion action occurs under the following circumstances:

- A digital line Media Module that is physically inserted into the system has ports currently administered for programmable terminals.

  If more than 20 port insertion requests are received within a few seconds, a global download request is started up as a background task. This action updates all programmable terminals instead of just those being inserted. This is done to avoid system overload for situations where there is massive board insertion. This could occur when connectivity to an EPN is reestablished after that EPN was down.

- A station port is added to the system by a "**add station**" or "**change station**" command.
- A TTI port is activated.

Audits

As part of periodic maintenance, the hardware status audit test queries programmable terminals to determine which levels and/or options are being used. If the reported values are not equal to the administered values, the system will initiate a terminal download action. This audit does NOT check the parameters used for softkeys.

Activation of TTI

A terminal is downloaded automatically when it is activated using the Terminal Translation Initialization feature. Therefore, no special user actions are required for TTI.

Plugging the station cord into a terminal does not automatically cause the terminal to be downloaded. If this terminal has factory defaults or if the terminal has been previously downloaded with parameters different than those desired, use one of the demand download actions described below to download the terminal.

Demand Download Actions

Busyout/Release Command

A maintenance demand busyout/release request for a station will cause the terminal to be downloaded regardless of its previous download status.

Feature Access Code

A Refresh Terminal Parameters Feature Access Code can be used to request a terminal download action. When this code is followed by a “#”, the programmable parameters for the current terminal are downloaded when the terminal goes on hook. When this code is followed by an extension, the programmable parameters for the specified station are downloaded.

This Refresh Terminal Parameters Feature Access Code is assigned on the second page of the “feature-access-codes” screen.

A confirmation is returned if the download request is accepted. A busy tone is returned if the request is made from a different station when the target station is off-hook.

The first three green call appearance LEDs on the 84xx 603x terminal will be turned on for three seconds if the station was successfully downloaded as a result of an entry of a Refresh Terminal Parameters Facility Access Code. This is not true for the 302B1 terminal.

There is no visible display on a station for the other background or demand download actions. As described below, the “status station” and “status attendant” screens can be used to check the download status of a specified terminal.

Status of Parameter Downloads

The “status station” and “status attendant” screens display the current download status of individual 84xx terminals in the Download Status field. The possible download states are:

Table 63: Download States

Status	Explanation
Complete	Terminal successfully downloaded sometime in the past.
Pending	System waiting to download the terminal. This may require the execution of a background periodic test which could take more than an hour. A demand download as described above may also be used to initiate an immediate download.
Not Applicable	Not a programmable terminal.

Possible reasons for terminal being not downloaded include:

- Terminal is off-hook.
- Terminal detected a bad checksum.
- Terminal detected a bad or missing EEPROM (refer to hardware error log).
- Terminal is busy programming data from a previous PROGRAM message.
- Terminal is in the Programming Disabled state.
- Terminal is in the Local Program Options Mode.
- Terminal is disconnected or out of service (use **status station** command).

Error Log Entries and Test to Clear Values

Table 64: Digital Line Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port *GGGVSpp* sh r 1
1 (a)	40987	None	WARNING	OFF	
1 (b)	1 to 20	None	WARNING	OFF	
18 (c)	0	busyout port *GGGVSpp*	WARNING	OFF	rel port *GGGVSpp*
130 (d)		None	WARNING	ON	test port *GGGVSpp* sh
257 (e)	40971	None			
513	0	Station (Digital) Audits Test (#17)	WARNING(o)	OFF	test port *GGGVSpp* sh r 6
767 (f)	40964	None	WARNING	OFF	
769 (g)	40963 40988	None	WARNING	OFF	
1026(o)		NONE	WARNING	OFF	
1281	Any	Station (Digital) Audits Test (#17)	WARNING	OFF	test port *GGGVSpp* sh r 4
1537 (h)	40968	None	WARNING	OFF	
2304 (n)		None			
2305 (i)	32770	None			
2305 (h)	40967	None			
2817(j)	Any	None		OFF	
3840 (k)	40965	None			
3840 (l)	40989	None			
3841 (m)	41029	None			

1 of 2

Table 64: Digital Line Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					
**Major alarms may be downgraded to Warning alarms based on the value used in the set options command.					
					2 of 2

Notes:

- (a) Could experience a noisy port or link. This is an off-board problem detected by the port circuit. Check for defective wiring, a defective voice terminal, or move voice terminal closer to the switch (in terms of feet of wire from the jack to the switch). If the problem still exists, replace the Media Module. Once the problem has been resolved, the alarm will be retired after a predetermined amount of time.
- (b) This Error Type and Aux Data will occur when at least 15 off-board problems have been detected with the link to the terminal. When an error with the link is detected, an on-board counter is incremented.

  The user could experience a noisy port or link. This is an off-board problem detected by the port circuit. Check for defective wiring, a defective voice terminal, or move voice terminal closer to the switch (in terms of feet of wire from the jack to the switch). If the problem still exists, replace the Media Module. Once the problem has been resolved, the alarm will be retired after a predetermined amount of time.
- (c) This error type is logged when the port in question is busied out by maintenance personnel. Make sure port is released from busyout via the **release port GGGVSpp** command.
- (d) This error type indicates that the Media Module has been removed or has been insane for more than 21 minutes. To clear the error, reinsert or replace the Media Module.
- (e) Problems transmitting to the voice terminal. This problem can be caused by defective wiring. Defective wiring can cause varying degrees of problems on different types of sets. Sets such as the 7410 appear to be more susceptible to wiring problems than other sets. This is usually an on-board problem and can be ignored if no user complaints are received.
- (f) This is an in-line event that produces this error type when a favorable response is received from running the Digital Line Electronic Power Feed Test (#11). No craft action is necessary. This alarm will be resolved with the passing of time.

- (g) With Aux Data 40963, this error type is a result of an overcurrent condition. With 40988, this error type indicates that the EPF circuit has been turned off due to an overcurrent condition.

  Once the problem has been resolved, it may take up to 1 hour for the alarm to clear due to “leaky bucket” strategy. If the problem cannot be resolved by one of the steps above, then replace the Media Module.

- (h) An in-line maintenance error has generated an off-board warning due to some problem with the link to the voice terminal. This can be ignored if no user complaints are received. Otherwise, make sure the voice terminal is connected, check for defective wiring, check for a defective voice terminal, and move voice terminal to a jack that is closer to the switch (in terms of feet of wiring between the jack and the switch). If the problem still exists, replace the Media Module. Once the problem has been resolved, the alarm will be retired after a predetermined amount of time.
- (i) This indicates that the station went off-hook while it was in the ready-for-service state. Use the **status station** command to determine the state of the station. The off-hook should have moved the station to ready-for-service. No craft action is necessary.
- (j) Port Level Hyperactivity—Fifty or more CCMS uplink messages were received from the port within ten seconds. The user is taken out of service for a short interval of time (default 30 seconds).
- (k) No terminal is connected to the Digital Line board. No maintenance action is required.
- (l) An uplink message has been logged indicating that the Electric Power Feed (EPF) is on with no load on it. No action is necessary.
- (m) The Media Module’s message buffer is full. This may be caused by having many display phones with heavy traffic connected to the Media Module. No action is necessary.
- (n) Internal system error. No action is necessary.
- (o) There is a problem with the voice terminal EEPROM. When the voice terminal is repaired the alarm will be resolved with the passing of time.

System Technician-Demanded Tests: Descriptions and Error Codes

Always investigate tests in the order presented in the table below. By clearing error codes associated with the *Voice and Control Channel Local Looparound Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 65: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
Digital Terminal Remote Looparound Test (#1201) **Note:** This Test ABORTS		X	D
Voice and Control Channel Local Looparound Test (#13) **Note:** This Test ABORTS		X	ND
Digital Line NPE Crosstalk Test (#9) **Note:** This Test ABORTS		X	ND
Digital Line Electronic Power Feed Test (#11)		X	ND
DIG-LINE Station Lamp Updates Test (#16)	X	X	ND
Station (Digital) Audits Test (#17)	X	X	ND

*D = Destructive; ND = Nondestructive

Digital Line Electronic Power Feed Test(#11)

MM711 boards provide power to the terminals. Therefore this will be an EPF restore test. The test procedure and its response is same as that of EPF. If the over current persists the power will be shut off automatically and an EPF_off_overcurrent message is sent uplink.

Table 66: TEST#11 Digital Line Electronic Power Feed Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.

1 of 2

Table 66: TEST#11 Digital Line Electronic Power Feed Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. Enter **display port GGGVSpp** to determine the station extension or attendant number of the port. Use **status station** or **status attendant** to determine the service state of the port. If the port is in use, wait until the port is idle before testing. Attendants are always in use (off-hook) if the handset is plugged in and the port is not busied out. If the port status is idle, then retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
	PASS	Electronic Power Feed Test passed. The message to turn on the power to the station was successfully sent to the port. Although this test will never actually return a FAIL result except for the **Internal system error** described above, it will log an error indicating the real results of the test. Check the Error Log for any entries with Error Types 767 or 769 after the test completes. If Error Type 767 appears in the Error Log, this indicates that the test sensed no problems with the power to the station. To verify that the station is powered up correctly, run a self-test on the station and check that all the feature buttons are operating. If Error Type 769 appears in the Error Log, this indicates some problem with the power to the station. Check for a short in the wiring, a damaged jack, a defective voice terminal, or an incorrect type of terminal.
Any	NO BOARD	The test could not relate the internal ID to the port. Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port. If the problem persists, replace the circuit pack.

2 of 2

DIG-LINE Station Lamp Updates Test (#16)

This test lights all lamps on the terminal as specified. The lamp updates will run only if the station is in-service. The status of the station is checked and the lamp updates are blocked from taking place if the station is not in the in-service state. This test does not affect the status of the Message Waiting lamp.

Table 67: TEST #16 DIG-LINE Station Lamp Updates Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
1	ABORT	This port may have been busied out by system technician. Look in the Error Log for Error Type 18 (port busied out) for this port. If this error type is present, then release the port via the **release station <extension>** command and run the test again. Make sure that the terminal is connected. Retry the command at 1-minute intervals a maximum of 5 times.
3	ABORT	Station may be in ready-for-service or out-of-service state. Use **status station** command to verify state of station. Make sure the terminal is connected. Retry the command at 1-minute intervals a maximum of 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. Use **display port GGGVSpp** to determine the station extension or attendant number of the port. Use **status station** or **status attendant** to determine the service state of the port. If the port is in use, wait until the port is idle before testing. Attendants are always in use (off-hook) if the handset is plugged in and the port is not busied out. If the port status is idle, then retry the command at 1-minute intervals a maximum of 5 times.
1392	ABORT	This port is currently a TTI port and the test will not execute on it. Verify that the port is a TTI port using either the **display port** command (the display shows that the port is a TTI port) or the **list config** command (the display shows a "t" for the port). If either **list config** or **display port** indicates that the port is *not* a TTI port, escalate the problem. If both commands indicate that the port is a TTI port, the abort is correct, and no action is necessary.
	FAIL	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.

1 of 2

Table 67: TEST #16 DIG-LINE Station Lamp Updates Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	The message to light all of the station lamps was sent successfully to the port. Observe the station lamps being lit when running the test. If all lamps do not light, the other Digital Line test results may indicate related problems that do not allow the lamps to light. Investigate by using other Digital Line port tests, and by examining the station, wiring, and connections.
Any	NO BOARD	The test could not relate the internal ID to the port. Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port. If the problem persists, replace the circuit pack.

2 of 2

Digital Station Audits Test (#17)

This is a series of six tests that are classified as audits. Messages are sent to the on-board microprocessor to perform the following tests. These audits run only if the station is in-service.

- Switchhook Inquiry Test — This is an update of the call records according to the Media Module's records. This inquiry is sent all the way to the voice terminal.
- Bad Scan Inquiry Test — A message is sent uplink which contains a count that is generated due to certain events relating to the link conditions. This can be an indication of communications problems between the Processor and Digital Port Media Module.
- For MM712, the status of the EPF is sent uplink. Possible conditions are: EPF-on-ok, EPF-off, and EPF-no-load.
- ID Request Test — A request is made to the station for its status. The station sends its configuration information and health information back. This information is checked and a pass/fail result is provided.
- Ringer Update Test — This updates the digital telephone ringer state according to the processor records.
- DTMF Administration Update Test — This is a message to the digital station to refresh the default value that causes the station to send touch- tones only in the primary information channel. This value is set initially when the station is put in-service and every time the station's state changes from other states to in-service.

Table 68: TEST#17 Station (Digital) Audits Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
1	ABORT	Switchhook audit timed out.
2	ABORT	ID request fails, health bit returned from voice terminal is bad. Make sure voice terminal is connected and repeat test. If test fails, replace voice terminal and repeat test.
3	ABORT	Look for Error Type 769 logged against DIG-LINE and follow the procedures in the associated footnote. If any additional problems are found, rerun the test.
4	ABORT	Internal system error Resolve any outstanding Media Module maintenance problems. Retry the command at 1-minute intervals a maximum of 5 times.
5	ABORT	Ringer update aborted due to station being in ready-for-service or out-of-service state.
6	ABORT	This port may have been busied out by system technician. Look in the Error Log for Error Type 18 (port busied out) for this port. If this error is present, release the port via **release station** Make sure that the terminal is connected. Retry the command at 1-minute intervals a maximum of 5 times.
1000	ABORT	System resources required for this test are not available.
1392	ABORT	This port is currently a TTI port and the test will not execute on it. Verify that the port is a TTI port using either the **display port** command (the display shows that the port is a TTI port) or the **list config** command (the display shows a "t" for the port). If either **list config** or **display port** indicate that the port is *not* a TTI port, escalate the problem. If both commands indicate that the port is a TTI port, the abort is correct, and no action is necessary.
2000	ABORT	Response to the test was not received in the allowable time period.
	FAIL	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.

1 of 2

Table 68: TEST#17 Station (Digital) Audits Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	Station Audits passed. This Digital Port Media Module is functioning properly. If complaints persist, investigate by using other port tests, and by examining the station, wiring, and connections.
Any	NO BOARD	The test could not relate the internal ID to the port. Check to ensure that the board translations are correct. Translate the board, if necessary. Use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board** command. This should re-establish the linkage between the internal ID and the port. If the problem persists, replace the circuit pack.

2 of 2

DIOD-TRK (DIOD Trunk)

Table 69: DIOD-TRK (DIOD Trunk)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
DIOD-TRK	MAJOR**	test port GGGvSpp l	DIOD Trunk
DIOD-TRK	MINOR	test port GGGvSpp l	DIOD Trunk
DIOD-TRK	WARNING	test port GGGvSpp l	DIOD Trunk
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			
A MAJOR alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options command and that at least 75 percent of the trunks in this trunk group are alarmed.			

Many trunk problems are caused by incorrect settings of parameters on the trunk group administration form. Settings must be compatible with the local environment and with parameter settings on the far-end. Refer to the Administration Manual for information on how to administer trunks. For the correct settings for administrable timers and other parameters on a country-by-country basis, see your local Avaya representative.

Services Supported by DIOD Trunks

Direct inward and outward dial (DIOD) trunks are 2-wire analog lines to the CO which support the following services:

- Both incoming and outgoing CO calls
- DID trunk
- DID trunk and 1-way outgoing DIOD

MM711 trunk Media Modules provide eight ports for loop-start CO trunks.

Loop Start Operation

Idle State: Tip = ground, Ring = CO Battery

Outgoing Call

1. PBX Off-Hook (Seize Message): Closes the Tip-Ring Loop CO Response: DC loop current + Dial tone.
2. PBX On-Hook (Drop Message): Open Tip-Ring loop, no loop current CO Response: CO goes to idle state (see Note).

Incoming Call

1. CO Applies Ringing Voltage PBX Response: Detect ringing current.
2. PBX Off-Hook (Answer Message): Close loop CO Response: Trip ringing, provide loop current.
3. PBX On-Hook (Drop Message): Open Tip-Ring loop, no loop current CO Response: CO goes to idle state (see Note).

Direct Inward Dialing (DID)

1. CO Applies Ringing Voltage.
   a. PBX Response: Detect ringing current and close loop.
   b. CO Response: Send DTMF digits.
   c. PBX Response: Acknowledge of Number dialed and open loop.
2. PBX Off-Hook (Answer Message): Close loop CO Response: Trip ringing, provide loop current.
3. PBX On-Hook (Drop Message): Open Tip-Ring loop, no loop current CO Response: CO goes to idle state (see Note).

Note:

CO does not normally provide an On-Hook (Disconnect) signal.

Error Log Entries and Test to Clear Values

Table 70: DIOD Trunk Error Log Entries

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port sh
15 (b)	any	Port Audit Update Test (#36)			
18	0	Busyout trunk *grp/mbr*	WARNING		release trunk
769 (a)	57392	None	MAJ/MIN/WRN**	ON	
1537 (f)					
2561 (a,d)	57345	None			
2817 (a,e)	57393	None			
3073 (a,c)	57376	None			
3585 (a,c)	57424	None			
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					
Major alarms on this MO may be downgraded to Warning alarms based on the value used in the set options command. If the Minor alarm is not downgraded by the **set-options values, the Minor alarm is upgraded to a Major alarm if 75 percent of the trunks in this trunk group are alarmed.					

Notes:

- (a) These are in-line errors that have no specific test associated with them. Refer to the following Table 71: DIOD Trunk Errors without Associated Tests on page 150 for an explanation and appropriate action.
- (b) This is a software audit error and does not indicate any hardware malfunction. Run the Short Test Sequence and investigate associated errors.
- (c) These errors cause the Dial Tone Test (#0) to run and are only considered a problem if the Dial Tone Test fails (in which case Error Type 1537 also appears). In this case, the trunk may be put in “Ready-for-Service” state (shown as “disconnected” by status command), which allows only incoming calls. Run the Dial Tone Test (#0) and follow its procedures.

  Aux data 57376—No loop current on incoming call

  Aux data 57424—No loop current on outgoing call

- (d) Single polarity ringing current—This error results from abnormal ringing current, but does not prevent the incoming call from being accepted. This error code is logged for information purposes only and does not cause additional testing to occur.
- (e) Late CO Trunk release—This indicates that the CO releases the trunk at least four minutes after the PBX dropped the call. This error code is only logged as an informational event and causes no other testing to occur.
- (f) This is a Dial-Tone Test.

Table 71: DIOD Trunk Errors without Associated Tests

Error Type	Aux Data	Description and Recommendation
769	57392	CO not releasing after call is dropped from PBX. After several occurrences, an off-board warning alarm is generated. Refer problem to CO.
2561	57345	Single polarity ringing current. This error results from abnormal ringing current, but does not prevent the incoming call from being accepted. One cause could be that the reverse current detector associated with the port is failing. (Will not be detected by any tests.) The other cause could be that normal current is not detected. In this case, neither incoming nor outgoing calls can be completed, and the dial tone test also fails. Check for other errors.
2817	57393	CO released the trunk at least four minutes after the PBX dropped the call. This error code is log only and causes no other testing to occur. No alarm is generated. Check for other errors.
3073	57376	No loop current on incoming call. The incoming destination has already answered and no loop current has been detected. If this is a hard fault, the dial tone test and all outgoing calls should also fail. Check for other errors.
3585	57424	No loop current on outgoing call. This error occurs on attempt to seize a loop or ground-start trunk for an outgoing call. An error occurs if loop current is not detected or the caller hangs up before it is detected. Busyout the affected port, and run a Long test. If Dial Tone Test #0 passes, ignore this error. Release the port.

System Technician-Demanded Tests: Descriptions and Error Codes

CAUTION:

Always investigate tests in the order they are presented in the table below. By clearing error codes associated with the *NPE Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence

Table 72: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** *This Test will abort with Error Code 1412*		X	ND
Dial Tone Test (#0) **Note:** *This Test will abort with Error Code 1412*		X	ND
Looparound and Conference Test (#33) **Note:** *This Test will abort with Error Code 1412*		X	ND
Audit Update Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Port Audit Update Test (#36)

This test sends updates of the CO port translation for all ports on the Media Module which have been translated. The update is non-disruptive and guards against possible corruption of translation data contained on the Media Module. No response message is expected from the Media Module once it receives translation updates. The port translation data includes: ground or loop start trunk, tone or rotary dialing trunk, rotary dialing inter-digit timing, network balance R/RC, and disconnect timing.

Table 73: TEST #36 Port Audit Update Test

Error Code	Test Result	Description/ Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.
2100	ABORT	Could not allocate the necessary system resources to run the test.
	FAIL	Internal system error. Retry the command at 1-minute intervals a maximum of 5 times.
	PASS	This test passed. Translation information was successfully updated on the Media Module. User-reported troubles on this port should be investigated by using other port tests and by examining trunk or external wiring. If the trunk is busied out, the test does not run, but returns PASS. To verify that the trunk is in-service: Enter **status-command** to verify that the trunk is in-service. If the trunk is in-service, no further action is necessary. If the trunk is out-of-service, continue to Step 2. Enter **release-trunk** command to put trunk back into in-service. Retry the test command.

ISDN-LNK (ISDN-PRI Signaling Link Port)

Table 74: ISDN-LNK (ISDN-PRI Signaling Link Port)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
ISDN-LNK**	MINOR	test port *GGGVSpp* l	ISDN-PRI Signaling Link Port
ISDN-LNK	WARNING	test port *GGGVSpp* sh	ISDN-PRI Signaling Link Port

*pp is *24* for 24-channel interfaces and *16* for 32-channel interfaces.

Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.

**For additional related information, see USD1-BD and MG-DS1 MOs.

The ISDN-PRI interface uses out-of-band signaling (as opposed to robbed-bit, in-band signaling) to transmit control messages between two endpoints. User information channels carry digitized voice and digital data and are known as bearer channels (B-channels). B-channels are assigned to DS1 ISDN trunks or PRI endpoints. Call control signaling for the B-channels is combined and carried over the separate ISDN-PRI Signaling Link Port D-channel.

The ISDN-PRI Signaling Link Port (ISDN-LNK) is a port on a MM710, which has a direct interface to the packet bus which carries D-channel messages to the processor. The associated B-channels can use ports on the same Media Module or ports on other MM710s.

Two types of DS1 interfaces exist:

- 24 DS0 channels on a 1.544 Mbps link
- 31 DS0 channels + 1 framing channel on a 2.048 Mbps link

On 24-channel interfaces, the B-channels may use any of the first 23 ports. The signaling link is assigned to the 24th port. On 32-channel interfaces, the DS1 ISDN Trunks (B-channels) may use any of ports 1 to 15 and 17 through 31. The signaling link is assigned to the 16th port. The 32nd channel (port 0) is used for framing. In NFAS configurations, the 24th or 16th ports on some of the DS1 Media Modules may be used for B-channels. Refer to ISDN-SGR for further information.

A problem with the ISDN-LNK will have an effect on all of the associated B-channels since without it no call control information can be conveyed to the far-end switch or terminal adapter. Stable calls may remain operational, but no new calls can be made. The ISDN-LNK in turn depends on the MM710 it resides on which provides the link to the processor. If there are problems with the ISDN-LNK, also investigate the MM710 Interface Media Module (MG-DS1).

Hardware Error Log Entries and Test to Clear Values

Table 75: ISDN-PRI Signaling Link Port Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port *GGGVSpp***
18 (a)	0	busyout port *GGGVSpp***	WARNING	OFF	release port *GGGVSpp***
130 (b)		None	WARNING	ON	test port *GGGVSpp***
1537 (c)	46210		WARNING	OFF	
1793 (d)					test board GGGVS l
3841 (f)	46211				

1 of 2

Table 75: ISDN-PRI Signaling Link Port Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
3842 (g)	46223				
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					
**pp is 24 for 24-channel interfaces and 16 for 32-channel interfaces.					
					2 of 2

Notes:

- (a) The D-channel is demand busied out. No calls can be made over this D-channel.
- (b) This Error Type indicates that the Media Module has been removed or has been insane for more than 11 minutes. To clear the error, reinsert or replace the Media Module.
- (c) Link error. This error occurs when the port receives an invalid frame over the D-channel. This error normally indicates an off-board problem usually related to transmission errors on the DS1 facility. Execute **list measurements ds1-log** for the MM710 Media Module on which the D-channel resides. If the MG-DS1 is reporting some errors, then the DS1 facility has experienced transmission problems which could have caused the ISDN-LNK to report a Link Error.

  If the MG-DS1 is not reporting errors, execute the long test sequence for the D-channel. Investigate any errors. If there are none, execute a long test sequence for the MM-DS1 Media Module. Investigate any errors.

  If no errors could be found by testing, the Link Error is probably not affecting service. However, if this Link Error continues to be logged, follow normal escalation procedures.
- (d) MG-DS1 Interface Media Module is out-of-service. Look for and resolve DS1-BD errors in the Hardware Error Log.
- (e) Bad DLCI error. This error occurs when a LAPD frame is received across the DS1 facility which contains a DLCI which does not have a valid entry in the on-board translation memory. This error normally indicates an off-board problem usually related to a broken endpoint or a state mismatch between a remote endpoint and the local call processing software. Maintenance will not start any testing or generate any alarms in response to this error.
- (f) Receive FIFO Overflow error. This error occurs when the Media Module detects an overflow of its receive buffers. If it occurs frequently, it may indicate a LAPD parameter mismatch between the two end-points of a packet switched connection. LAPD should be able to recover from this problem, but it may degrade the performance of the LAN Bus. Maintenance will not start any testing or generate any alarms in response to this error.

System Technician-Demanded Tests: Descriptions and Error Codes

The command to test the ISDN-LNK MO is **test port** GGGVSpp where pp is 24 for 24-channel interfaces and 16 for 32-channel interfaces.

Table 76: System Technician-Demanded Tests

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) This test will ABORT with error code 1412,			
Signaling Link Board Check (#643)	X	X	ND
Signalling Port LAN Loopback Test (#939) This test will ABORT with error code 1412.			
*D = Destructive; ND = Nondestructive			

Signaling Link Board Check (#643)

This test checks the health of the MM710 Interface transporting the ISDN-PRI Signaling Link Port

Table 77: Test #643 Signaling Link Board Check *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal System Error Retry the command at 1-minute intervals for a maximum of 5 times. If the test continues to abort, escalate the problem.
1700	ABORT	Rollabout video abort. The PRI terminal adapter associated with this D-channel port is detached from the Media Module. This is normal when the rollabout video feature is enabled. To complete a test on this port, do one of the following: Re-attach the disconnected PRI terminal adapter Disable the rollabout video feature on this board by entering **change ds1 GGGVSpp** and set the field labeled “Alarm when PRI Endpoint Detached?” to “y.”

1 of 2

Table 77: Test #643 Signaling Link Board Check *2 of 2*

Error Code	Test Result	Description/ Recommendation
8	FAIL	The MM710 is not in-service. Check the Hardware Error Log for entries logged against DS1 MM and consult the DS1 Interface Media Module Maintenance documentation for repair procedures.
	PASS	The MM-DS1 Interface Media Module transporting the ISDN-PRI Signaling Link Port is in-service.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

ISDN-SGR (ISDN-PRI Signaling Group)

Table 78: ISDN-SGR (ISDN-PRI Signaling Group)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
ISDN-SGR	MINOR	test sig-group *grp#*	ISDN-PRI Signaling Group
ISDN-SGR	WARNING	test sig-group *grp#*	ISDN-PRI Signaling Group

**grp#* is the signaling group number (1-166); the test sequence can be either short or long.

An ISDN-PRI Signaling Group is a collection of B-channels for which a given ISDN-PRI Signaling Channel Port (D-channel) carries signaling information. B-channels carry voice or data and can be assigned to DS1 ISDN trunks (ISDN-TRK) or PRI endpoint ports (PE-BCHL).

Note:

Throughout this discussion the term B-channels refers to ISDN-TRKs or PE-BCHLs, depending on the application under investigation.

The MM710 Interface Media Module, which has a direct interface to the packet bus, is required for D-channel signaling. There are two types of DS1 interfaces:

- 24 DS0 channels on a 1.544 Mbps link
- 31 DS0 channels + 1 framing channel on a 2.048 Mbps link

The following discussion describes 24-channel interface signaling groups. The 32-channel interface works the same way, except that only port number 16 is used for signaling instead of port number 24. Ports 1 through 15 and 17 through 31 are used for B-channels. The 32nd channel (port 0) is always used for framing.

ISDN-PRI D-channel signaling can be combined with a group of B-channels in three basic ways:

- Facility-associated signaling (FAS)
- Nonfacility-associated (NFAS) simplex signaling
- NFAS duplex signaling

In a FAS signaling group, the 24th port of the DS1 MM Interface Media Module carries D-channel signaling for up to 23 B-channel ports on the same Media Module.

In an NFAS signaling group, the 24th port of one DS1 MM Interface can carry D-channel signaling for B-channels on several other DS1 Media Module as well, including TN767s and TN464Bs. The 24th port on the other Media Modules can be used for B-channels. A D-channel in an NFAS group can signal for B-channels on a total of 20 DS1 Media Modules.

NFAS duplex signaling provides increased reliability, which is highly desirable since NFAS permits the D-channel to signal for many more B-channels. NFAS Duplex allows the administration of a backup D-channel which remains in a standby state until the active D-channel goes down. If the active D-Channel does go down, the backup D-Channel takes over and provides signaling for all the B-channels in the signaling group.

The operation of the entire ISDN-PRI signaling group depends on several other entities: the ISDN-PRI signaling channel ports, the MG-DS1 Interface Media Module on which the D-channels reside and the system link that is carried over the packet bus to the processor. When there are problems with the ISDN-PRI signaling group, also investigate ISDN-LNK, MG-DS1, and SYS-LINK.

Error Log Entries and Test to Clear Values

Table 79: ISDN-PRI Signaling Group Error Log Entries

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any		test sig-group *grp#*
1 (a)	Any	None			
257 (b)	Any	None			test sig-group *grp#*
513 (c)	Any	None			test sig-group *grp#*
769	Any	Primary Signaling Link Hardware Check (#636)			test sig-group *grp#*
1025	Any	Secondary Signaling Link Hardware Check (#639)			test sig-group *grp#*
1793 (d)	Any	Layer 2 Status (Test #647)	WARNING	OFF	test sig-group *grp#*
2049 (e)	Any	Layer 2 Status (Test #647)	WARNING	OFF	test sig-group *grp#*
2305 (f)	Any	Remote Layer 3 Query (Test #637)	MINOR	OFF	test sig-group *grp#*
3585 (g)	Port number	None			
3842 to 3942(h)	Port number	None			

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

Notes:

- (a) This switch sent a message to the far-end switch or terminal adapter, and the far-end did not respond in the allotted time. Possible causes include link failure and congestion or outage at the far-end. The Aux Data field contains Layer 3 protocol information used by internal counters.

If no other symptoms are present, no action is required. If Layer 3 communication is down, there should be indications in the form of alarms and errors for link components. Check out other errors against ISDN-SGR, ISDN-TRK, and other hardware components on the link.

There is no test to clear these errors. The error counter is decremented by 1 every 15 minutes.

- (b) This error indicates that the primary signaling channel connection has been lost for more than 90 seconds. If a secondary signaling channel does not exist or is not in-service, the associated B-channels will be placed in the ISDN Maintenance/Far-End state. The B-channels will not be usable for outgoing calls, although incoming calls will still be accepted. The switch will automatically attempt to recover the signaling link. Pay particular attention to the results of Test #636 (Primary Signaling Link Hardware Check) in the test sequence. When the link does recover, the B-channels will be negotiated back to the In-Service state and their alarms will be retired.

  When this error occurs, the state of the Signaling Group is changed to out-of-service (verify using the **status sig-group** command).

- (c) This error indicates that the secondary signaling channel connection has been lost for more than 90 seconds. If the primary signaling channel is not in-service, B-channels will be placed in the ISDN Maintenance/Far-End state. The B-channels will not be usable for outgoing calls, although incoming calls will still be accepted. The switch will automatically attempt to recover the signaling link. Pay particular attention to the results of Test #639 (Secondary Signaling Link Hardware Check) in the test sequence. When the link does recover, the B-channels will be negotiated back to the In-Service state and their alarms will be retired.

  When this error occurs, the state of the Signaling Group is changed to out-of-service (verify using the **status sig-group** command).

- (d) This error indicates a failure of the Layer 2 Query Test for the primary signaling channel.

- (e) This error indicates a failure of the Layer 2 Query Test for the secondary signaling channel.

- (f) This error indicates a failure of Test #637, the Remote Layer 3 Query. A specific message was sent to the far-end switch, and it did not respond within the allotted time. Investigate elements of the ISDN PRI D-channel(s) (ISDN-LNK) for both this switch and the Far-end switch. If Test #637 fails twice in a row, the B-channels will be alarmed and made unavailable for outgoing calls (although incoming calls will still be accepted). When Test #637 succeeds and the Far-end switch starts responding properly, the DS1 ISDN Trunk (B-channels) will be placed back into normal operation and their alarms will be retired.

- (g) A SERV or SERV ACK ISDN D-channel message has been received by a non-US-type interface (country option other than 1 on the DS1 administration form). However, these messages are used only for duplex NFAS signaling which is supported only by country protocol 1.

  Thus, there may be a mismatch in administration between the local and far-end switches. Consult with the customer's network provider to determine whether the D-channel is set up correctly on the far-end switch.

- (h) These Error Types are used to report certain error messages received by the ISDN-PRI Signaling Group for one of its associated B-channels. The aux data field shows for which B-channel (port number) the message was received.

  The error code generated equals 3840+*x*, where *x* is a Cause Value defined by the ISDN PRI Specification. Note that there is no Test to Clear Value for these Error Types; selected ISDN cause values are placed in the log when they are received, but no direct action or alarming is performed solely in response to receiving them. They provide added data that may prove useful when tracking down obscure networking and routing problems. The following table provides more information:

Table 80: Descriptions and Recommendations for Error Types 3842-3942 ***1 of 4***

Error Code	Description	Recommendation
3842	A request has been made to use a transit network or common carrier that cannot be accessed.	From the Media Module and port number (in the Aux Data field), determine the trunk group against which the error was reported. Check all routing patterns containing this trunk group for validity of interexchange carriers requested (IXC field).
3843	No route to destination. Request received to route call through a transit network that is recognized but not allowed to carry the call or not able to serve the destination.	

1 of 4

Table 80: Descriptions and Recommendations for Error Types 3842-3942 *2 of 4*

Error Code	Description	Recommendation
3846	The far-end switch has indicated that the B-channel (trunk) is not acceptable for use in the call for which it was requested.	This could indicate an administration problem (for example, the local switch and the far-end switch have different B-channels administered), or could reflect the occurrence of a normal race condition (for example, the local switch has requested use of a B-channel which the far-end switch had just reserved for use on another call). From the Media Module and port number (in the Aux Data field), determine the trunk group against which the error was reported. Use the **status trunk** command for the indicated trunk. Refer to the “DS1 ISDN Trunk Service States” and “ISDN-PRI Trunk Service States” sections of ISDN-TRK for recovery suggestions.
3858	Similar to Error Type 1. The switch sent an ISDN message to the far-end switch or terminal adapter which did not respond in the allotted time.	Follow same recommendations as for Error Type 1.
3878	The far-end switch has indicated that the network is not functioning correctly and that the condition may last a relatively long period of time (for example, immediately re-attempting the call may not be successful).	From the Media Module and port number (in the Aux Data field, determine the trunk group against which the error was reported. Consult with the network provider to determine the nature and expected duration of the out of service condition. Consider modifying all routing patterns containing this trunk group, to route calls around the network which is out of service.

2 of 4

Table 80: Descriptions and Recommendations for Error Types 3842-3942 *3 of 4*

Error Code	Description	Recommendation
3890	A request to use a network service (e.g., ISDN) has been denied. Administration somewhere on the network has indicated that the requested service has not been subscribed to or purchased for this trunk.	This could be a local administration problem only, or a mismatch between the local administration and that of the network provider. From the Media Module and port number (in the Aux Data field), determine the trunk group against which the error was reported. Display the trunk group form: If the trunk group is Call-by-Call (Service Type is “cbc”), check all routing pattern forms containing this trunk group to see if the Service/Feature fields contain the correct network services purchased for this trunk. If the trunk group is not Call-by-Call, check that the Service Type field contains the single network service purchased for this trunk. If local administration appears correct, consult with the customer and/or the network provider to determine the services that the customer has subscribed to for this trunk group.
3892	Protocol detail; may offer a clue if customer is having ISDN calls denied with an unexpected intercept tone.	If customer is complaining of unexpected intercept tones when accessing ISDN trunks or PRI endpoints and no other cause can be found, escalate the problem and provide the next tier with this Error Log information.
3894	Protocol detail; may offer a clue if customer is having ISDN calls denied with an unexpected intercept tone.	First, eliminate any transitory state mismatch problems by issuing the **test port GGGVSpp** command for the trunk port shown in the aux data field. Test #256 (Service State Audit) is the important test in the sequence. If this passes satisfactorily, yet the customer continues to complain of unexpected intercept tones when accessing ISDN trunks or PRI endpoints and no other cause can be found, escalate the problem and provide the next tier with this Error Log information.
3902	FRANCE ONLY: Service not authorized.	
3903	Service or option not available, unspecified. This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.	

3 of 4

Table 80: Descriptions and Recommendations for Error Types 3842-3942 *4 of 4*

Error Code	Description	Recommendation
3905	Protocol detail; may offer a clue if customer is having ISDN calls denied with an unexpected intercept tone.	If customer is complaining of unexpected intercept tones when accessing ISDN trunks or PRI endpoints and no other cause can be found, escalate the problem and provide the next tier with this Error Log information.
3906	Protocol detail; may offer a clue if customer is having ISDN calls denied with an unexpected intercept tone.	If customer is complaining of unexpected intercept tones when accessing ISDN trunks or PRI endpoints and no other cause can be found, escalate to the problem and provide the next tier with this Error Log information.
3909	A request to use a network service has been made, but the network has rejected the request because the requested service is not implemented.	Follow the recommendations listed above for Error Type 3890.
3910	Only restricted digital BC available.	
3919	Service or option not implemented, unspecified. Used when no other cause in this class applies.	
3928	A call was denied because of a basic incompatibility between the type of call and either the facilities selected by the routing pattern or the called user itself.	This error might be helpful as a clue if the customer complains of receiving unexpected intercept tone after accessing ISDN trunks or PRI endpoints. Determine the trunk group from the Media Module and port number (in the aux data field) and then check the BCC fields of the pertinent routing patterns. Also, investigate whether or not the calling and called endpoints are compatible (for example, some ISDN switches may not allow a voice station to call a data extension).
3942	Timer expiry: T310 time-out, no answer to CALL PROCEEDING.	

4 of 4

System Technician-Demanded Tests: Descriptions and Error Codes

Always investigate tests in the order presented in the table below when inspecting errors in the system. By clearing error codes associated with the *Primary Signaling Link Hardware Check*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 81: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
Primary Signaling Link Hardware Check (#636)	X	X	ND
Secondary Signaling Link Hardware Check (#639)	X	X	ND
Layer 2 Status Test (#647)	X	X	ND
Remote Layer 3 Query Test (#637)	X	X	ND
*D = Destructive; ND = Nondestructive			

Primary Signaling Link Hardware Check (#636)

The ISDN-PRI Signaling Group D-Channel port depends on the health of the Media Module on which it resides. This test will fail if there are problems with either the ISDN-PRI Primary D-channel port or the MM-DS1 Media Module. If there are problems with the ISDN-PRI Primary Signaling Channel port (ISDN-LNK), also investigate the Media Module.

Table 82: Primary Signaling Link Hardware Check (#636) *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
1700	ABORT	Rollabout video abort. The PRI terminal adapter associated with the primary D-channel port is detached from the Media Module. This is a normal abort when the rollabout video feature is enabled. To complete test on this port, either: Re-attach the disconnected PRI terminal adapter, or Disable the rollabout video feature on this board by entering **change ds1 GGGVSpp** and set field “Alarm when PRI Endpoint Detached?” to “y.”

1 of 2

Table 82: Primary Signaling Link Hardware Check (#636) *2 of 2*

Error Code	Test Result	Description/ Recommendation
8	FAIL	There is a problem with the MM710 or the ISDN-PRI Signaling Channel (D-Channel). No ISDN trunk or PRI endpoint calls can be made until the problem is resolved. Consult the procedures for the MM710 and the ISDN-PRI Signaling Channel (ISDN-LNK).
	PASS	The basic physical connectivity of the primary D-channel is intact and functional. One might try this test repeatedly to ensure the link is up and to uncover any transitory problems.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

Remote Layer 3 Query (#637)

This test will query the far-end switch or terminal adapter to determine if the signaling connection is functioning properly at Layer 3. It will select a B-channel in the in-service or maintenance service state and send an ISDN Layer 3 SERVice message, which requires a response from the far end (similar to performing Test #256 on an ISDN trunk. The test will not be performed if there are no B-channels in an appropriate ISDN service state (as when none are administered or they are all out of service).

Note:

The service state can be displayed by using the **status trunk <trunk group/ trunk member>** or **status pri-endpoint** command.

As is the case with Test #256 for an ISDN trunk, a PASS only indicates that a message was composed and sent to the far-end switch or terminal adapter. The ISDN PRI Specification allows up to 2 minutes for a response. Check the Error Log for ISDN-SGR (ISDN-PRI Signaling Group) errors of type 2305 for evidence of a Remote Layer 3 Query failure.

Tests #639 and #636 check the health of the D-channels and DS1 Interface Media Modules. This test goes one step further by checking the communication path from the processor, and on to the far-end switch or terminal adapter. A special ISDN message is sent to the far-end switch or terminal adapter, which must respond within a specified amount of time. This test is designed to ensure that the communication path between the switch and the far-end is up and operational, and that the two endpoints can properly exchange ISDN control messages.

Table 83: TEST #637 Remote Layer 3 Query *1 of 2*

Error Code	Test Result	Description/ Recommendation
1006	ABORT	There are no associated B-channels in an ISDN “in-service” or “maintenance” service state. This is a NORMAL ABORT. Administer or release an ISDN trunk or PRI endpoint before retrying the test. For an ISDN trunk, use the **status trunk** group#/member# command to verify the ISDN trunk state. For a PRI endpoint use **status pri-endpoint** extension. Then, retry this test when at least one B-channel is in the “in-service” or “maintenance” states.
1113	ABORT	The signaling channel is down. Therefore, no messages can be sent to the far-end switch or terminal adapter. Examine the results of Tests #636 and #639 and follow recommendations provided there.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.
2500 or none	ABORT	Internal system error OR Administration Problem Determine if any B-channels are administered. If there are none, then this is a normal ABORT, since this test cannot run unless at least one B-channel is administered. If at least one B-channels is administered, there is an internal system error. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Internal system error. See description of ABORT with error code 2500.

1 of 2

Table 83: TEST #637 Remote Layer 3 Query *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	A message was composed and sent to the far-end switch or terminal adapter. The ISDN PRI specification allows up to 2 minutes for a reply. Check the Error Log for ISDN-SGR (ISDN-PRI Signaling Group) for errors of type 2305 for evidence of a Remote Layer 3 Query failure. If no new errors were logged since this test was run, then this switch and the far-end switch or terminal adapter can exchange call control messages. If there is still a problem with a particular ISDN trunk or PRI endpoint, busyout the trunk and run the long test sequence, paying particular attention to the results of Test #258 (ISDN Test Call).
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.
		2 of 2

Secondary Signaling Link Hardware Check (#639)

The ISDN-PRI Signaling Group D-Channel port depends on the health of the MM710 on which it resides. This test will fail if there are problems with either the ISDN-PRI Secondary D-channel port or the MM-DS1 Media Module. This test will abort if a Secondary D-channel is not administered for the signaling group. If there are problems with the ISDN-PRI Secondary Signaling Channel port (ISDN-LNK), also investigate the MM710.

Table 84: TEST #639 Secondary Signaling Link Hardware Check

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
1132	ABORT	The Secondary D-Channel is not administered for this Signaling Group. This is a NORMAL ABORT. Only a Primary D-Channel must be administered for a Signaling Group.
8	FAIL	There is a problem with the MM710 or the ISDN-PRI Secondary Signaling Channel (D-Channel). No ISDN trunk or PRI endpoint calls can be made until the problem is resolved. Consult the procedures for the MM710 and the ISDN-PRI Signaling Channel (ISDN-LNK).
	PASS	The basic physical connectivity of the Signaling Group's Secondary D-channel is intact and functional. Try this test repeatedly to ensure the link is up and to uncover any transitory problems.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

Layer 2 Status Test (#647)

The Layer 2 Status Test checks the layer 2 status of the ISDN-PRI Signaling Channel (D-channel). This test will fail if there is a hardware failure or a facility problem, or if the primary and secondary ISDN-PRI D-channels are not administered correctly.

The Primary and Secondary Signaling Link Hardware tests (test 637 and 639) and the Remote Layer 3 Query test (test 637) will detect most problems caused by hardware failures or incorrect administration. However, the Layer 3 test (test 637) cannot detect end-to-end transmission problems with the Standby D-channel since Layer 3 messages are not sent on the standby channel.

The SYS-LINK Maintenance Object reports Layer 2 ISDN-PRI D-channel problems. The Layer 2 Query test is provided to detect D-Channel Layer 2 failures and generate an associated Warning alarm independent of the hardware configuration used for the D-channels.

Table 85: TEST #647 Layer 2 Status Query Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
1132	ABORT	Internal system error: The port location for the primary ISDN-PRI D-channel is not known. This condition should not be possible since an administered DS1 Media Module must be specified when a Signaling Group is administered: Retry the command at one minute intervals a maximum of five times.
1134	ABORT	Internal system error: The associated DS1 Media Module is not administered. This condition should not be possible since an administered DS1 Media Module must be specified when a Signaling Group is administered. Retry the command at one minute intervals a maximum of three times.
2500	ABORT	Internal system error: Retry the command at one minute intervals a maximum of five times.
1	FAIL	Layer 2 of the primary signaling channel is down: Examine the results of the Primary Signaling Test (#636) and follow recommendations provided there. If test #636 passes, the Layer 2 Query test may still fail if the Signaling Channel at the far end has not been administered correctly or if the Signaling Channel has been busied out. Verify that the Primary Signaling Channel (D-channel) at the far end has been administered correctly. Verify that the DS1 port used for the Primary D-channel has not been busied out at the far end.

1 of 2

Table 85: TEST #647 Layer 2 Status Query Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
2	FAIL	Layer 2 of the secondary signaling channel is down. Examine the results of Secondary Signaling Link Hardware Test (#639) and follow recommendations provided there. If tests #639 passes, the Layer 2 Query test may still fail if the Signaling Channel at the far end has not been administered correctly or if the Signaling Channel has been busied out. Verify that the Secondary Signaling Channel (D-channel) at the far end has been administered correctly. Verify that the DS1 port used for the Secondary D-channel has not been busied out at the far end.
3	FAIL	Both the primary and secondary are down. Examine the results of the Primary and Secondary Signaling Link Hardware Tests (#636 and #639) and follow recommendations provided there. If tests #636 and #639 pass, the Layer 2 Query test may still fail if the Signaling Channel at the far end has not been administered correctly or if the Signaling Channel has been busied out. Verify that the Primary and Secondary Signaling Channel (D-channel) at the far end has been administered correctly. Verify that the DS1 port used for the Primary and Secondary D-channels has not been busied out at the far end.
	PASS	The Primary Signaling Channel is up and, if administered the Secondary Channel is up.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

ISDN-TRK (DS1 ISDN Trunk)

Table 86: ISDN-TRK (DS1 ISDN Trunk)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
ISDN-TRK**	MAJOR*	test port GGGVSpp l	DS1 ISDN Trunk
ISDN-TRK	MINOR	test port GGGVSpp l	DS1 ISDN Trunk
ISDN-TRK	WARNING	test port GGGVSpp l	DS1 ISDN Trunk
Note: For Avaya G350 Media Gateway systems you must consult local records for the location and designation of the equipment rack where the G350 is mounted.			
*For additional repair information, see also DS1-BD for TN767 ports and MM710.			
A MAJOR alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options command.			

Note:

Many trunk problems are caused by incorrect settings of parameters on the trunk group administration form. Settings must be compatible with the local environment and with parameter settings on the far-end. See "*Administrator's Guide for Avaya Communication Manager*, 555-233-506", for the correct settings for administrable timers and other parameters on a country-by-country basis.

Note:

Throughout this section, the term DS1 refers to the MM710 Media Module.

A DS1 ISDN trunk is a 64 Kbps bearer channel used to transmit digitized voice or data traffic. These trunks, or B-channels, use a separate channel, the D-channel for call-control signaling. This mode of operation is known as out-of-band signaling, as opposed to in-band robbed-bit signaling, in which signaling is carried in the same channel as the voice or data traffic. One D-channel, or ISDN signaling link (ISDN-LNK), carries signaling messages for several B-channels, forming an ISDN signaling group (ISDN-SGR).

A B-channel may be a port on a MM710 series DS1 Media Module.

Two types of DS1 interfaces exist:

- 24 DS0 channels on a 1.544 Mbps link
- 31 DS0 channels + 1 framing channel on a 2.048 Mbps link

On 24-channel interfaces, any of the first 23 ports on the DS1 Media Modules can be a B-channel. On the MM710, the 24th port may be used as a B-channel or as a D-channel depending on the type of ISDN-PRI signaling group (FAS or NFAS) implemented on the Media Module. For more details, refer to ISDN-SGR. The signaling for these B-channels is done over a D-channel located on a MM710.

On 32 channel interfaces, any of ports 1-15 and 17-31 on the DS1 interface Media Module can be a B-channel. The 16th port may be used as a B-channel or as a D-channel depending on the type of ISDN-PRI signaling group (FAS or NFAS) to which it belongs. For more details, refer to ISDN-SGR and “MG-DS1 (DS1 Interface Media Module)” in this chapter.

For interfaces using country protocol 1 on the DS1 Media Module administration form (including US), the signaling protocol used for the maintenance of the B-channel is defined by the ISDN-PRI specification. For interfaces using country protocols other than 1, the signaling protocol used for the maintenance of the B-channel is defined by the CCITT ISDN-PRI Specification.

There are five possible service states for a B-channel. the service state is negotiated with the far-end switch, changes over time, and may have a far-end and near-end components. The service state is initialized to out-of-service/Far-End and an attempt is made to negotiate it to in-service.

The ISDN-PRI Specification defines the possible SERVICE STATES for a B-channel. The service state is negotiated with the far-end switch, changes over time, and may have a far-end or near-end component. The service state is initialized to the Out-Of-Service/Far-End state and an attempt is made to negotiate it to In-Service.

Note:

The service state of a particular DS1 ISDN Trunk B-channel can be displayed by issuing the **status trunk** *trunk group/trunk member* system technician command.

When a call is present, the specification defines the permissible call states as well. There are tests in the short and long test sequences for DS1 ISDN Trunk designed to audit these states and ensure agreement between both ends of the PRI connection.

Alarming Based on Service States

A warning alarm is logged against a DS1 ISDN B-channel trunk when it is placed in the Maintenance/Far-End or Out-Of-Service/Far-End states, during which the trunk is unusable for outgoing calls. When a warning alarm is present, use **status trunk** group#/member# command to determine the exact state. Other alarms can be diagnosed by using the short and/or long test sequences. Note that an ISDN B-channel trunk can be placed in a Far-End service state by either action taken by the far-end switch or by failure of the far-end switch to respond. For example, if the far-end does not respond to a Remote Layer 3 Query (Test #637 for ISDN-SGR), the associated DS1 ISDN trunk B-channels will be placed in the Maintenance/Far-End service state.

As a port on a DS1 Media Module (MG-DS1), and as part of a signaling group dependent on a D-channel (ISDN-LNK) for signaling, operation of the ISDN-TRK is dependent on the health of these other maintenance objects.

DS1 ISDN Trunk Service States

The **status trunk** command displays the following possible service states for ISDN trunks. Table 87: Service States on page 174 gives recommended procedures for each state.

- In-Service (INS)

  The B-channel is in its normal operating state.

- Out-of-Service/Far-End (OOS/FE)

  A B-Channel is initialized to this state when administered. The switch sends messages to the far-end to negotiate the B-channel into service. If the far-end does not respond to the messages within a certain time period, then the service state remains out-of-service and maintenance will periodically resend the messages. The trunk is unusable for incoming and outgoing calls.

- Out-of-Service/Near-End (OOS/NE)

  This is the state of the trunk when the NPE Crosstalk Test fails or when the trunk is busied out by system technician. In this state, the trunk is unusable for incoming or outgoing calls. No messages are sent to the far-end until the signaling link comes back into service or the trunk is released by system technician.

- Maintenance/Far-End (MTC/FE)

  This state is reached when the far-end does not respond to messages sent over the signaling link for a particular trunk after a certain amount of time. This state is different from OOS/FE since the signaling link must have initially been up and the B-Channels in-service. The switch will periodically send messages to the far-end to try to negotiate the trunk (B-channel) into service. The trunk is unusable for outgoing calls but will service incoming call requests from the far-end. Note that transitions into MTC/FE do not drop stable calls. Therefore, if the service state changes from in-service to MTC/FE, then stable calls are unaffected.

- Maintenance/Near-End (MTC/NE)

  The trunk (B-channel) is in this state if the signaling channel (ISDN-LNK) is busied out by system technician. The trunk (B-channel) is also temporarily in this state if system technician has used a **test trunk** *trunk group/trunk member long* command. This command will execute the ISDN-PRI test call. This test will change the state of the trunk member to MTC/NE for the duration of the test unless a call request comes in from the far-end. In that case, the test would abort. Note that transitions into MTC/NE do not drop stable calls. In this state, the B-Channel is not usable for new incoming or outgoing calls.

- Pending States

  In addition to one of the above components, the service state may have a *pending* component, indicating that the switch is waiting for a reply from the far-end. These service states remain in effect until either a response is received or the allotted waiting time expires.

  - Pending-in-Service

    The near-end is waiting for a response from the far-end to a B-channel maintenance message requesting that the B-channel be transitioned to in-service.

  - Pending-Maintenance

    This state is supported only by systems using country protocol 1 (including US). The near-end is waiting for a response from the far-end to a maintenance message requesting that the B-channel be transitioned to the maintenance service state.

- Call Activity States

  The in-service state also has a call activity component.

  - Active

    A call is connected over the B-channel (for example, *in-service/active*).

  - Idle

    There is no call currently on the B-channel (for example, *in-service/idle*).

Table 87: Service States *1 of 2*

Service State	Alarm*	Possible Cause	Possible Solution
out-of-service/NE	Warning	Trunk is demand busied out.	Enter **release trunk** grp#/ mbr#.
	None	DS1 or MM-DS1 Media Module lost its signal.	Is the Media Module or cable removed? Is the far-end switch restarting? Check Media Module using procedures in MG-DS1.
out-of-service/FE	Warning	Unadministered far-end	Administer corresponding trunk on far-end switch.
	Warning	The far-end trunk is busied out.	Check the status of the far-end switch.
pending-in-service, pending-maint	None	Maintenance message was sent and the switch is waiting up to 2 min. for a reply from the far-end.	Wait 2 minutes and check service state after the pending state has cleared.

1 of 2

Table 87: Service States *2 of 2*

Service State	Alarm*	Possible Cause	Possible Solution
maint-NE	None	ISDN test call in progress (**test trunk long** and **test isdn-testcall** commands)	Wait several minutes for test to finish and check status again.
	None	System link has been busied out by command.	Check link status. Release link with **release link** *link#*.
maint-FE	Warning	Signaling channel has been down for over 90 sec.	Consult ISDN-SGRP and/or ISDN-LNK. Far-end signaling channel may be busied out, or the far-end switch may currently be restarting.
	Warning	Repeated failure of far end to respond to messages.	Maintenance software will periodically try to resend messages. You can speed the process with **test trunk** grp#/mbr# and/or **test signaling-gr** #.
	Warning	The far-end trunk is being tested.	Check status of the far-end switch. Wait for testing to finish.
in-service	None	Normal operating state	

*ISDN-TRK alarms; alarms against other objects may also be present.

2 of 2

Error Log Entries and Test to Clear Values

Table 88: DS1 ISDN Trunk Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test port *GGGVSpp*
1(a)	Any	None			test port *GGGVSpp*
15(b)	Any	Audit and Update Test (#36)			

1 of 2

Table 88: DS1 ISDN Trunk Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
18	0	busyout trunk *grp/mbr*			release trunk *grp/mbr*
19(c)	0	None			
129(d)		None	WARNING	OFF	test port *GGGVSpp*
130(e)		None	WARNING	ON	test port *GGGVSpp*
257(f)	Any	None			test port *GGGVSpp*
513(g)	Any	None	WARNING	OFF	test port *GGGVSpp*
769(h)	Any	None			test port *GGGVSpp*
1025	0	None			
1793(i)	Any	None			test port *GGGVSpp*
3073(j)	Any	Service State Audit (#256)			test port *GGGVSpp*
3585(k)	Any	None			none
3841(l)	Any	None	WARNING	OFF	None

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

**Major or minor alarms may be downgraded to Warning alarms based on the value used in the set options command.

2 of 2

Notes:

- (a) These Error Types indicate a disagreement between this switch and the switch at the other end of the trunk connection with regard to the ISDN call state of the DS1 ISDN Trunk. This switch will automatically try to recover by clearing the call, (that is, call will be torn down). You can use the **status trunk** group#/member# command to determine the state of the trunk.

  When running the Short Test Sequence of tests, pay close attention to the results of the Call State Audit Test (#257).

- (b) Software audit error and does not indicate a hardware malfunction. Run the Short Test Sequence and investigate associated errors.

- (c) Possible protocol mismatch or far-end may be out-of-service.

  Many trunk problems are caused by incorrect settings of parameters on the trunk group administration form. Settings must be compatible with the local environment and with parameter settings on the far-end. A DS1 ISDN trunk is a 64 Kbps bearer channel used to transmit digitized voice or data traffic. These trunks, or B-channels, use a separate channel, the D-channel for call-control signaling. This mode of operation is known as out-of-band signaling, as opposed to in-band, robbed-bit signaling, in which signaling is carried in the same channel as the voice or data traffic. One D-channel, or ISDN signaling link (ISDN-LNK), carries signaling messages for several B-channels, forming an ISDN signaling group (ISDN-GRP). A B-channel may be a port on DS1 MM. Two types of DS1 interfaces exist: (1) 24 DS0 channels on a 1.544 Mbps link or (2) 31 DS0 channels + 1 framing channel on a 2.048 Mbps link. For additional maintenance information, see also MG-DS1.

- (d) The far-end switch changed its ISDN service state to either *out-of-service* or *maintenance*. This may be a temporary condition due to testing of that trunk by the far-end, or a hardware problem with the trunk. Outgoing calls will not be allowed over the trunk. To investigate the status of the trunk, use the **status trunk** group#/member# command.

- (e) This Error Type indicates that the Media Module has been removed or has been insane for more than 11 minutes. To clear the error, reinsert or replace the Media Module.

- (f) These Error Types indicate a disagreement between this switch and the switch at the other end of the trunk connection with regard to the ISDN service state of the DS1 ISDN Trunk. This switch will automatically try to recover by performing a service state audit. You can use the **status trunk** group#/member# command to determine the state of the trunk.

  When running the Short Test Sequence, pay close attention to the results of the Service State Audit Test (#256).

- (g) This trunk is not recognized by the far-end switch. Investigate the trunk administration for both switches and make changes as necessary.

- (h) An unexpected SERVICE or SERVICE ACK was received. Possibilities include:

  - Translations conflict
  - Protocol differences
  - ESS may be using NI3 protocol which is not currently implemented in Communication Manager
  - B-channel negotiation problem (glare)

- (i) This error indicates a failure of the DS1/MM-DS1 Interface Media Module. When running the Short Test Sequence, the results of the Signaling Link State Check Test (#255) are important.

- (j) Service State Audit attempt failed (see Test #256). The trunks will not be usable for any outgoing calls (although incoming calls will be accepted) until the test passes and the trunk state is changed to in-service (use **status trunk** group#/member# to investigate trunk status).

- (k) Error Type 3585 appears when the switch receives an ISDN RESTART message for an ISDN trunk. Calls are cleared with the RESTART message. Therefore, this Error Type may be associated with a dropped call report from a user.

  The following Aux Data values for Error Type 3585 represent the trunk's ISDN call state at the time the unexpected request to restart the channel was received from the remote switch. This information can be useful if dropped calls (cutoffs) are reported by users of the ISDN-PRI trunks.

  The meanings of Aux Data values are shown below; ignore any others.

  Table 89: Aux Data Values

Aux Data	Cause
0	A idle trunk received a restart.
10	A call in a stable, talking state was cleared unexpectedly by the far-end with an ISDN RESTART message. This state is called the "active" state.
4 7 8 260 263	A call that has not reached the active state, but has at least reached a ringing state, was cleared unexpectedly by the far-end with an ISDN RESTART message.
1 3 6 9 265	A call that has not yet reached a ringing state was cleared unexpectedly by the far-end with an ISDN RESTART message.
11 12 19 531 267 268	A call that was in the process of clearing anyway has been cleared by the far-end with an ISDN RESTART message. If this condition occurs frequently, it may mean that the far-end is attempting to clear trunks that it thinks are in a "hung" state. The RESTART message brings the trunk to an idle condition.

- (l) An ISDN trunk selected by the near-end has been rejected 10 times by the far-end without a successful call. This may indicate a service state mismatch between the near-end and far-end for this trunk that is effecting the end user (that is, customer receives unexpected intercept tones when accessing ISDN trunks). This may indicate that the ISDN trunk is not administered on the far-end.

  The Aux field contains the physical name of the ISDN trunk in decimal. Then, verify that the far-end has this trunk administered.

  The Warning alarm will be retired automatically whenever an outgoing or incoming call that uses this trunk is answered by the called endpoint. If problems persist, then busy-out the ISDN trunk to take it out of the hunt group.

System Technician-Demanded Tests: Descriptions and Error Codes

Always investigate tests in the order presented in the table below when inspecting errors in the system. By clearing error codes associated with the *NPE Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 90: System Technician-Demanded Tests: MG-DS1

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** This Test ABORTS when run on a Avaya G350 Media Gateway system.		X	ND
Conference Circuit Test (#7) **Note:** This Test ABORTS when run on a Avaya G350 Media Gateway system.		X	ND
Audit and Update Test (#36)	X	X	ND
Signaling Link State Check Test (#255)	X	X	ND
Service State Audit Test (#256)	X	X	ND
Call State Audit Test (#257)	X	X	ND
ISDN Test Call Test (#258) **Note:** This Test ABORTS when run on a Avaya G350 Media Gateway system.		X	ND
*D = Destructive, ND = Non-destructive			

Audit and Update Test (#36)

This test sends port level translation data from switch processor to the DS1 interface Media Module to assure that the trunk's translation is correct. The port audit operation verifies the consistency of the current state of trunk kept in the DS1 interface Media Module and in the switch software.

Table 91: TEST #36 Audit and Update Test

Error Code	Test Result	Description/ Recommendation
1018	ABORT	Maintenance is disabled on this trunk. Enable maintenance by entering "y" in the "Maintenance Tests?" field on page 2 of the **change trunk-group** form.
	ABORT	Internal system error
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	Could not allocate the necessary system resources to run this test.
	FAIL	Test failed due to internal system error. Retry the command at 1-minute intervals for a maximum of 5 times.
	PASS	Trunk translation has been updated successfully. The current trunk states kept in the DS1 interface Media Module and switch software are consistent.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

Signaling Link State Check Test (#255)

The DS1 ISDN Trunk depends on the health of the appropriate MM710 Interface Media Module. It also depends on the ISDN-PRI D-channel (ISDN-LNK) trunk. This test checks the status of those critical elements.

Table 92: TEST #255 Signaling Link State Check Test

Error Code	Test Result	Description/ Recommendation
None	ABORT	Internal system error
0	ABORT	
1114	ABORT	The signaling link is in a transitional state. Retry the command at 1-minute intervals for a maximum of 5 times.
1018	ABORT	Maintenance is disable on this trunk. Enable maintenance by entering “y” in the “Maintenance Tests?” field on page 2 of the **change trunk-group** form.
4	FAIL	There is a problem with the signaling channel. Consult the procedures for the ISDN-PRI Signaling Group (ISDN-SGRP). Further information may also be obtained by consulting the procedures for the ISDN-PRI Signaling Channel (ISDN-LNK).
8	FAIL	There is a problem with the DS1 interface Media Module. Consult the procedures for the appropriate DS1 interface Media Module (MG-DS1).
	PASS	The signaling link hardware is OK.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

Service State Audit (#256)

As noted in the general description for DS1 ISDN Trunk, these trunks may be in one of several service states. This test performs a Service State Audit with the far-end switch.

For interfaces using country protocol 1 (including the US) the Service State Audit executes in all trunk service states. A message is sent to the far-end switch to ensure that both sides agree on the service state. A PASS for this test simply means that the message has been successfully sent. Two minutes are allowed for a reply. If no reply is received within that 2 minute window, the message is sent out again. If that attempt fails, an Error Type 3073 will be logged and the switch will attempt another Service State Audit every 15 minutes. If the trunk was initially in-service, it is placed in the maintenance/far-end state. No outgoing calls will be placed over this trunk, but incoming calls will be accepted. If an incoming call is presented with the trunk in such a state, a Service State Audit is immediately be attempted (the switch does not wait for the 15-minute cycle, but tries to recover immediately).

For interfaces not using country protocol 1, the Service State Audit executes only if the trunk is in the out-of-service/far-end state. A message is sent to the far-end switch to attempt to bring the trunk back into the in-service state. A PASS for this test simply means that the message has been successfully sent. Two minutes are allowed for a reply. If no reply is received within that two minute window, the message is sent out again. If again no response is received within two minutes, the trunk remains in the out-of-service/far-end state. The switch will attempt another Service State Audit after an hour has passed.

To investigate the service state of the DS1 ISDN Trunk, use the **status trunk** group#/member# command.

Table 93: TEST #256 Service State Audit Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
1000	ABORT	Resources required to run this test were not available. The port may be on a valid call or initializing. Use **status station** or **status trunk** to determine when the trunk is available for testing. Check the results of Test #255.
1018	ABORT	Maintenance is disabled on this trunk. Enable maintenance by entering “y” in the “Maintenance Tests?” field on page 2 of the **change trunk-group** form.
1113	ABORT	The signaling link has failed, so the system cannot send any messages on behalf of this trunk. Check the results of Test #255 and consult procedures for ISDN-SGR (ISDN-PRI Signaling Group) in this chapter.

1 of 2

Table 93: TEST #256 Service State Audit Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
1114	ABORT	The signaling link is in a transitional state. Retry the command at 1-minute intervals for a maximum of 5 times.
1116	ABORT	The trunk is not in the out-of-service/far-end state, which is required to run this test on systems using a country protocol other than 1.
1117	ABORT	A service state audit message is outstanding. Wait 2 minutes and then try again.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1113	FAIL	The signaling link has failed; the system cannot send any messages on behalf of this trunk. Consult procedures for ISDN-SGR (ISDN-PRI Signaling Group) and ISDN-LNK (ISDN Signaling Link Port).
	FAIL	Internal system error Retry the command at 1-minute intervals for a maximum of 5 times.
	PASS	Wait 4 minutes and then check the Error Log for any new errors of type 3073. If there are none, then both sides of the ISDN connection agree on the service state; the negotiation succeeded. If there is a new 3073 error, then the negotiation failed (the far-end switch twice failed to respond within 2 minutes). The switch will automatically retry every 15 minutes. If the trunk was initially in-service, it is now placed in the maintenance/ far-end state. Incoming calls will be accepted, but no outgoing calls can be originated. If an incoming call is presented, another Service State Audit will be immediately performed in an attempt to put the DS1 ISDN Trunk in the proper state.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

Call State Audit Test (#257)

If a call is active on the trunk, the switches on both sides of the connection should agree on the ISDN state of the call, as defined in the ISDN Protocol Specification. This test audits internal call state data by querying the far-end switch as to the ISDN state of the call. It can be helpful when trying to clear a hung call. If the internal call state data on the near-end switch is different than that of the far-end switch, then *the call will be torn down.*

As with Test #256 (Service State Audit), a PASS simply means that an appropriate message was composed and sent to the far-end switch. The ISDN Specification allows up to 2 minutes for a reply. If a reply is not received within the 2 minute window, a protocol time-out violation will be recorded in the error log against the associated signaling channel (ISDN-LNK, Error Type 1).

Table 94: TEST #257 Call State Audit Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
1018	ABORT	Maintenance is disable on this trunk. Enable maintenance by entering “y” in the “Maintenance Tests?” field on page 2 of the **change trunk-group** form.
1019	ABORT	An audit is already in progress. Wait 2 minutes and try again.
1113	ABORT	The signaling link has failed, so the system cannot send any messages on behalf of this trunk. Check the results of Test #255 (Signaling Link State Check).
1114	ABORT	The signaling link is in a transitional state. Retry the command at 1-minute intervals for a maximum of 5 times.
1116	ABORT	The trunk is in an out-of-service ISDN service state. A call cannot be present if the trunk is in an ISDN out-of-service state, so a call state audit would be inappropriate. No action necessary. (Use the **status trunk** group#/member# command to investigate the ISDN state of the trunk).
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	Internal system error Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 2

Table 94: TEST #257 Call State Audit Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	This switch sent a call state auditing message to the far-end switch to verify the state of the call active on this trunk. If a call state mismatch is found, then the call will be torn down within two minutes. If no call was active, then no message was sent.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

MED-GTWY (MEDIA GATEWAY)

Table 95: MED-GTWY (Media Gateway)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
MED-GTWY	MAJOR	test board GGGVS	MEDIA GATEWAY

Note: You must consult local records for the location and designation of the equipment rack where the media gateway is mounted.

This maintenance object monitors the H.248 link to the media gateway. It logs errors when the Keep Alive messages that are exchanged between the server and media gateway fail. These messages indicate the status of the H.248 link between the two. If the keep alive messages are active all is well, if not an error is logged.

Error log entries and test to clear values

Table 96: MED-GTWY error log entries

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
1(a)		None	MAJOR	OFF	
257 (b)		None	MAJOR	OFF	
513 (c)		None	MAJOR	ON	
769 (d)		None	MINOR	OFF	

Notes:

- **(a) Error Type 1**: this error type indicates a failure of the H.248 link keep alive messages between the server and the G350. This is an indication that the LAN or the platform is down.
- **(b) Error Type 257**: If the server is an LSP, this error type indicates that at least one Media Gateway is registered with the LSP.
- **(c) Error Type 513**: this error type indicates that there is a problem on the G350. Log on to the G350 and check the error log for problems using the G350 CLI.
- **(d) Error Type 769**: this error type is a transient error, indicating that the link has unregistered with the G350. If the G350 re-registers, the alarm is resolved. If the *link loss delay timer* on the primary server expires, Error Type 1 is logged.

System Technician-Demanded Tests: Descriptions and Error Codes

There are no System Technician-Demanded Tests associated with this MO.

MG-ANA (ANALOG MM711, MM714)

Note:

For more information, refer to the MO XXX-BD section of this document. In addition, refer to the AN-LN-PT MO and to the CO-TRK MO.

Table 97: MG-ANA (ANALOG MM711, MM714)

MO Name (in Alarm Log)	For Location	Full Name of MO
MG-ANA	GGGVSPP	ANALOG MEDIA MODULE
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.		

The Avaya MM711 Analog Trunk and Line Media Module provides 8 ports, any of which may be administered as one of the following:

Table 98: MM711 Analog Trunk and Line Media Module – port administration

Function	Group Type	Trunk Type	LED MWI
Central Office trunk (CO)	co fx wats	loop start ground start	
CAMA/E911 trunk	cama	loop start	
Direct Inward Dialing (DID) trunk	did	wink start immed start	
Analog Line on-or-off premises	n/a	n/a	with/ without MWI

The Avaya MM714 Media Module has 8 ports. Ports 1-4 can only be configured as lines, and ports 4-8 can only be configured as trunks.

The MM 711 Analog Media Module supports eight analog interfaces allowing the connectivity of Loop Start, Ground Start, Analog DID trunks, and 2-wire analog Outgoing CAMA E911 trunks. As well, the MM711 Analog Media Module allows connectivity of analog, tip/ring devices such as single line telephones, modems, or group 3 fax machines. Each port may be configured as either a trunk interface or a station interface. Also included is support for caller ID signaling, ring voltage generation for a variety of international frequencies and cadences and administrable line termination styles.

Analog modems are supported on the G350 only in limited configurations, in which the modem call stays within a single Media Gateway. If the modem is connected to an MM711 Analog Media Module, and the call goes to either a) another modem on an MM711 within the same Media Gateway, or b) the PSTN through an analog, T1/E1, or BRI trunk on the same Media Gateway, the call will succeed.

If the modem is connected to an MM711, and the call goes to a) a modem or trunk on a different Media Gateway or port network, or b) an IP trunk, the call will most likely fail. Modem calls are not supported even between Media Gateways in a stacked configuration.

The MM711 Analog Trunk and Line Media Module does not support Neon Lamp Message Waiting Indication (MWI). No maintenance of the terminal connected to the Neon Analog Line Media Module is performed.

System Technician-Demanded Tests: Descriptions and Error Codes

CAUTION:

Always investigate tests in the order they are presented in the table below when inspecting errors in the system. By clearing error codes associated with the NPE Crosstalk Test, for example, you may also clear errors generated from other tests in the testing sequence.

Table 99: Order of Investigation

Order of Investigation	Short Test Sequence	Long Test Sequence	Reset Board Sequence	D/ND*
NPE Audit Test (#50) **Note:** *This test will abort with Error Code 1412.*		X		ND
Ringing Application Test (#51) Aborts with code 1412				
Control Channel Looparound Test (#52)	X	X		ND
SAKI Sanity Test (#53)		X	D	
NEON Test (#220) Aborts with code 1412				
*D = Destructive; ND = Nondestructive				

For hardware error log entries and for more information on the tests listed in the table above refer to “MO XXX-BD (common port Media Module)” maintenance object documentation.

MG-BRI (BRI Trunk Media Module MM720 and MM722)

Table 100: MG-BRI (BRI Trunk Media Module MM720 and MM722)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
MG-BRI	MINOR	test board *GGGVM**	MO_MG_BRI

*. Where *GGG* is the administered Media Gateway number, *VM* is the Media Module slot number (V1, if no S8300, through V4), and, if required in a port command, *pp* is a two-digit port number (01 - 08).

The MM720 and MM722 BRI Media Modules contain eight, 4-wire ports that interface to the network at the ISDN S/T reference point over two 64 Kb/s channels (B1 and B2) and over a 16Kb/s signaling (D) channel.

LEDs

The three LEDs on the Media Module faceplate indicate board status. When illuminated, the red LED indicates a board failure or a major or minor on-board alarm, the green LED indicates that testing is in progress, and the amber LED indicates that the board is in use.

ISDN Interface Reference Points

Figure 11: Integrated Trunk-Side BRI, ISDN Interface Reference Points on page 190 shows, for a generic integrated trunk-side BRI, the ISDN Interface Reference Points. Table 101: ISDN Interface Reference Point definitions on page 190 gives definitions for the generic ISDN Interface Reference Points.

Figure 11: Integrated Trunk-Side BRI, ISDN Interface Reference Points

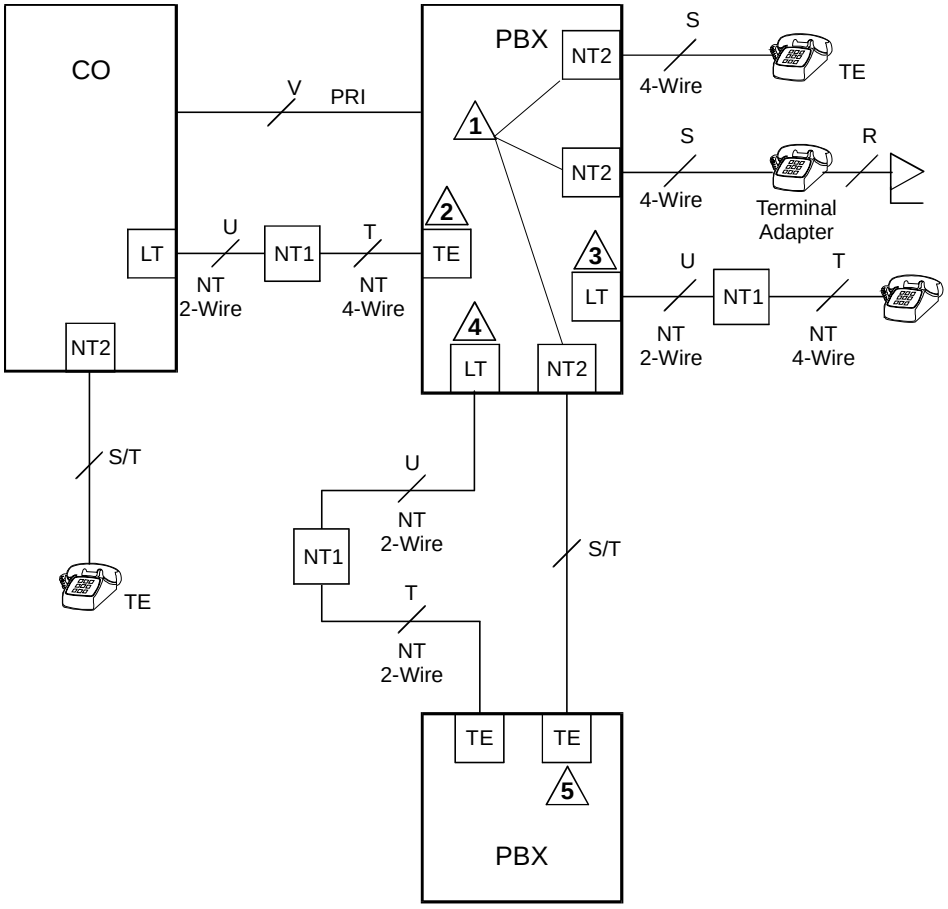


Table 101: ISDN Interface Reference Point definitions *1 of 2*

LT	Logical Terminal
V	Primary Rate user/network (asymmetrical) trunk interface. The ECS is capable of acting as the user or as the network side of this 1.544 - or 2.048-Mbps interface.
R	Interface between Terminal Equipment and Network Termination
S	Basic Rate network-side 4-wire line interface
S/T	4-wire Basic Rate connection to a Network Termination*.
T	4-wire Basic Rate interface to a Network Termination.†
TE	Terminal Equipment

1 of 2

Table 101: ISDN Interface Reference Point definitions *2 of 2*

U	Basic Rate network-side 2-wire line interface.
1	TN556B ISDN-BRI 4-Wire S/T-NT Line (A-law)
2	TN 2185 ISDN-BRI 4-Wire S Interface (Trunk Side)
3	TN2198 ISDN-BRI 2-Wire U Interface
4	TN2198 ISDN-BRI 2-Wire U Interface
5	TN 2185 ISDN-BRI 4-Wire S Interface (Trunk Side)

2 of 2

*. Network Termination 2 (NT2), that terminates Layer 1 and higher layers. PBXs, LANs, and terminal controllers typically provide NT2 functionality including protocol handling and multiplexing for Layers 2 and 3.

†. Network Termination 1 (NT1), that terminates Layer 1 and monitors maintenance, performance, timing, power transfer, multiplexing, and multi-drop termination with contention resolution.

Error Log Entries and Test to Clear Values

Table 102: Error Log Entries and Test to Clear Values *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test board GGGVM sh r 1
1 (a)	Any	None	MINOR	ON	
257 (b)	65535	Control Channel Loop Test (#52)	MINOR	ON	test board GGGVM r 20
513 (c)	4352 to 4357		None	ON	
769 (d)	4358				
1025 (e)		NPE/NCE Audit Test (#50)	None	ON	
1291 (f)	4359	Clear Error Counters (#270)	MINOR	ON	

1 of 2

Table 102: Error Log Entries and Test to Clear Values *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
3586 (g)			MINOR	OFF	
3840(h)	4096 to 4101				
3842 (i)	46095				
3843 (j)	46097				

2 of 2

*. Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

Notes:

- Error Type 1 – The circuit pack stopped functioning or is physically removed from the system.

  This alarm logs approximately 11 minutes after removing the circuit pack and/or the SAKI Sanity Test (#53) fails.

  If the circuit pack is not in the system, insert a circuit pack in the same slot as the error indicates. See note (g).

- Error Type 257 – Transient communication problems between the switch and this circuit pack. Execute the **test board GGGVM** command and refer to the repair procedures for the Control Channel Loop Around Test (#52).

- Error Type 513 – On-board hardware failure. Aux data values correspond to the following detected errors:

Aux Value	Detected Error
4352	External RAM error
4353	Internal RAM error
4355	ROM Checksum error
4357	Instruction set error

  Reset the circuit pack with the **busyout board GGGVM** and **reset board GGGVM** commands. When reset, the circuit pack executes a set of tests to detect the presence of any of the faults listed above. Detection of one of these errors during initialization causes the circuit pack to lock-up and appear insane to the system. See the repair procedure in Note ().

- Error Type 769 – The circuit pack detects a program logic error. While no action is required, this error can lead to other errors against this circuit pack.
- Error Type 1025 – The circuit pack cannot update and read back NPE/NCE memory. This error can be ignored, but may lead to other errors against this circuit pack.
- Error Type 1291 – The MM720 and MM722 BRI Media Modules notify maintenance software that they have detected a parity error while accessing their dynamic RAM (that stores the board's translation information and downloadable application firmware). Maintenance software resets the circuit pack.
- Error Type 3586 – The SPE software detects an excessive number of up-link messages from the TN2185 board within a certain time period. To prevent the faulty board from flooding the switch with data, the switch software takes the board out of service and alarms it. The switch software also tells the Archangel to ignore up-link messages from the board.

  When the board is alarmed due to this error, the switch software periodically puts the board back in service and tells the Archangel to process up-link messages from the board. If the problem still exists, the software takes the circuit pack out of service again. If the circuit pack does not exhibit the problem for a certain time period, then maintenance software resolves the alarm and the circuit pack is left in service.
- Error Type 3840 – The circuit pack received an inconsistent down-link message (a bad header, port number, data, sub-qualifier, or logical link) over the Control Channel.
- Error Type 3842 – The board is receiving data from the bus faster than it can distribute the data to its endpoints, causing the FIFO RAM buffer to overflow. This error can occur occasionally due to the statistical sizing of the buffers. If it occurs frequently, it may indicate a LAPD parameter mismatch. LAPD should recover from this problem, but it may degrade the performance of the LAN bus.

  When this error is reported, maintenance reads and clears the board counter and logs the problem in the maintenance error log.
- Error Type 3843 – Bad translation RAM detected, but the call continues by using another translation location. The circuit pack reports this error when it cannot update NPE/NCE memory and read it back. This error is not service-affecting and can be ignored, but can lead to other types of errors against this circuit pack.

System Technician-Demanded Tests: Descriptions and Error Codes

When inspecting errors in the system, always investigate tests in the order listed below. By clearing error codes associated with the *Control Channel Loop Around Test,* for example, you may also clear errors generated from other tests in the testing sequence.

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
Control Channel Loop-Around Test (#52)	X	X	ND
NPE/NCE Audit Test (#50) Aborts with Error Code 1412		X	ND
LAN Receive Parity Error Counter Test (#595)		X	ND
SAKI Sanity Test (#53)		X	D

*. D = Destructive; ND = Nondestructive

Control Channel Loop Around Test (#52)

Refer to the repair procedure described in the “XXX-BD (Common Port Circuit Pack)” section.

NPE /NCE Audit Test (#50)

This test will abort with ABORT CODE 1412. This test is an audit that sends network update messages to various ports on a board. Since the Media Server does not handle network connections for the Media Gateway, this test is not intended to be run.

SAKI Sanity Test (#53)

CAUTION:

This test is destructive.

Refer to the repair procedure described in the “XXX-BD (Common Port Circuit Pack)” section. This test is only run as a part of a reset board procedure.

LAN Receive Parity Error Counter Test (#595)

The test reads and clears a circuit pack’s LAN Receive Parity Error Counter.

MG-DCP (Digital Line Media Module)

DIG-LINE maintenance monitors and tests ports on digital line Media Modules and the hardware connected to those ports for lines administered as a digital station. Media Gateway-level maintenance is covered by “MG-DCP” whose strategy is described in the “XXX-BD (Common Port Media Module)” section.

Table 103: MG-DCP (MM712 and MM312 Digital Line Media Module)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
MG-DCP	MIN	test board GGGVS sh	Digital Line Media Module
MG-DCP	WRN	test board GGGVS sh	Digital Line Media Module
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			

Note:

Refer to XXX-BD (Common Port Media Module) for Media Module level errors. See also “DIG-LINE” for related line information.

MG-DS1 (DS1 Interface Media Module)

Table 104: MG-DS1 (DS1 Interface Media Module)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
MG-DS1	MAJOR	test board GGGVS sh	DS1 Interface Media Module
MG-DS1	MINOR	test board GGGVS l	DS1 Interface Media Module
MG-DS1	WARNING	test board GGGVS sh	DS1 Interface Media Module
NOTE: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			

Echo Cancellation

The MM710 Media Module features an integrated echo canceller. Echo cancellation supports channels carrying voice and is not intended for channels that support data. The MM710 has the capability to detect modem tone and turn off echo cancellation accordingly for the duration of a data call. Echo cancellation on the MM710 is administrable per channel. The echo cancellation circuitry on a given MM710 is driven by administrable parameters.

The MM710 Media Modules are intended for use with ATM, IP, wideband, or other complex services which are likely to have problems with echo.

The echo cancellation circuitry on a given MM710 is a right-to-use feature activated on the System-Parameters Customer-Options form. Also on this form is a field `Maximum Number of DS1 Boards with Echo Cancellation` that indicates the number of DS1 boards on which echo cancellation is activated for a specific customer.

The DS1 MEDIA MODULE form for the MM710 Media Module has fields to support echo cancellation: `Echo Cancellation?`, `EC Direction`, and `EC Configuration`. The `Echo Cancellation?` field displays only if the Echo Cancellation feature has been activated on the **system-parameters customer-options** form by entering a `y` in the `DS1 Echo Cancellation?` field. The `EC Direction` and `EC Configuration` fields do not display unless the user has entered `y` in the `DS1 Echo Cancellation?` field.

- EC Direction determines the direction from which echo will be eliminated, ether inward or outward.
- EC Configuration is the set of parameters that will be used when cancelling echo. This information is stored in firmware on the MG-DS1 Media Module.

Echo cancellation is turned on or off on a trunk group basis using the **change trunk-group** command. If the TRUNK GROUP field, `DS1 Echo Cancellation?` is set to `y`, echo cancellation will be applied to every MM710 trunk member in that trunk group. The echo cancellation parameters used for a given trunk member are determined by the Echo Cancellation Configuration Number administered on the **DS1 Media Module** form for that specific trunk's board.

Note:

It is not necessary to busyout a port or trunk group to change the `DS1 Echo Cancellation?` field on page 2 of the **change trunk-group** form; however, the modified setting will not take effect until one of the following occurs:

- Port is busied-out/released
- Trunk group is busied-out/released
- Test trunk group is executed
- Periodic maintenance runs

Echo cancellation on the MM710 is selectable per channel, even though it is administrable on a trunk group basis. For example, if all but two ports on a MM710 need to have echo cancellation applied, those two ports must be put in a trunk group where the `DS1 Echo Cancellation` field is set to n. The remaining ports will be in a trunk group(s) where the `DS1 Echo Cancellation` field is set to y. A user will have the ability to cancel echo coming from the network (far-end echo) or coming from the switch (near-end echo).

MM710 DS1 Media Module

The MM710 Universal DS1 Interface Media Module provide an interface to the DS1 facility, and are designed to support 24 DS0 channels on a 1.544 Mbps DS1 link, or 32 DS0 channels on a 2.048 Mbps link. The DS0 channels can be administered as trunks to other switches, lines to off-premises stations, ports to line-side PRI terminating devices, or ports to other line-side non-PRI terminating devices. (DS0 channels on the MG-DS1 can only be administered as trunks to other switches.) For more information on how MM710 ports can be used, see the maintenance objects (MOs): ISDN-SGR, ISDN-TRK, ISDN-LNK, TIE-DS1, CO-DS1, DID-DS1, and WAE-PT.

Note:

The MM710 provides Echo Cancellation, and in addition, the MM710 firmware may be updated using the firmware download feature.

The MG-DS1 maintenance strategy includes logging in-line errors reported by the MG-DS1 Media Module, running tests for error diagnosis and recovery, and raising or clearing maintenance alarms.

MM710 Media Modules support the following:

- Digital Tie, CO, and DID trunks
- DS1 off-premises (OPS) lines
- Narrowband and wideband access endpoint ports
- ISDN-PRI trunks and accompanying signaling channel
- PRI endpoint ports (PE-BCHL) and accompanying signaling channel

Each trunk, line, or endpoint has its own maintenance strategy, but all depend on the health of the MG-DS1 Interface Media Module. Refer to the following MOs for details: TIE-DS1, CO-DS1, DID-DS1, OPS-LINE, ISDN-TRK, ISDN-LNK, ISDN-SGR, WAE-PT and PE-BCHL.

Media Module Administration and Options

The DS1 configuration for each Media Module is administered on the **DS1 Media Module** form. `Bit Rate` is set to 1.544 Mbps for 24-channel systems, and 2.048 Mbps for 32-channel systems. `Country Protocol` is used to drive layer 3 protocol decisions based on PRI specifications specific to a given country (not those related to specific features). This Country Protocol is independent of the `Country` parameter administered on the **country-options system-parameters** form. Different MG-DS1 Media Modules may be administered with different Country Protocols, allowing the switch to act as a gateway between two incompatible ISDN-PRI implementations (for example, between two different countries). US systems use country protocol 1.

Echo cancellation is administered in part by administering an echo cancellation plan. Currently, DS1 Echo Cancellation Plan 4 is the default plan.

CAUTION:

The DS1 Echo Cancellation Plan 1 uses a 96ms echo tail and introduces **6db of loss** for additional cancellation. Because no digital facilities have ever introduced loss, this is an unexpected side effect of the Plan 1 echo cancellation feature. Since services personnel might not expect to find it there, services might try to change the loss plan to compensate, which can lead to other problems.

Error Log Entries and Test to Clear Values

Table 105: DS1 Interface Media Module Maintenance Error Log Entries *1 of 3*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test board GGGVS
1(a)	0	Media Gateway removed or SAKI Test (#53)	MIN/WRN**	ON	
18(b)	0	busyout board GGGVSpp	WARNING	OFF	release board GGGVS
23(c)	0		WARNING	OFF	add ds1 GGGVS
125(d)	none 3	None	MIN/WRN**	ON	
257	65535	Control Channel Loop Test (#52)	MINOR	ON	test board GGGVS l r 20

1 of 3

Table 105: DS1 Interface Media Module Maintenance Error Log Entries *2 of 3*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
257(e)	Any	None			
513(f)	Any		MIN/WRN**	ON	
514(g)	46086		MIN/WRN**	ON	
769(h)	46085		MIN/WRN**	ON	
770(i)	46096		MIN/WRN**	ON	
1281	Any	Loss of Signal Alarm Inquiry Test (#138)	MIN/WRN**	OFF	test board GGGVS
1320	Any	Loss of Signal Alarm Inquiry Test (#138)	MIN/WRN**	OFF	test board GGGVS
1321	Any	Loss of Signal Alarm Inquiry Test (#138)	MIN/WRN**	OFF	test board GGGVS
1322	Any	Loss of Signal Alarm Inquiry Test (#138)	MINOR	ON	test board GGGVS
1323	Any	Loss of Signal Alarm Inquiry Test (#138)	MIN/WRN**	OFF	test board GGGVS
1324	Any	Loss of Signal Alarm Inquiry Test (#138)	WARNING	OFF	test board GGGVS
1400, 1401(j)	Any	Loss of Signal Alarm Inquiry Test (#138) and Echo Cancellation Test (#1420)	MINOR	ON	test board GGGVS
1537(k)	46082		MIN/WRN**	ON	
1538(l)	Any		MIN/WRN**	ON	
1793	Any	Blue Alarm Inquiry Test (#139)	MAJ/MIN / WRN ***	OFF	test board GGGVS
1794	Any	Blue Alarm Inquiry Test (#139)	MAJ/MIN / WRN***	OFF	test board GGGVS
1795	Any	Blue Alarm Inquiry Test (#139)	MAJ/MIN / WNG***	OFF	test board GGGVS
2049	Any	Red Alarm Inquiry Test (#140)	MIN/WRN**	OFF	test board GGGVS

2 of 3

Table 105: DS1 Interface Media Module Maintenance Error Log Entries *3 of 3*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
2305	Any	Yellow Alarm Inquiry Test (#141)	MIN/WRN**	OFF	test board GGGVS
2306	Any	Yellow Alarm Inquiry Test (#141)	MIN/WRN**	OFF	test Board GGGVS
2561	Any	Major Alarm Inquiry Test (#142)	MIN/WRN**	OFF	test board GGGVS
2817		Minor Alarm Inquiry Test (#143)	MIN/WRN**	OFF	test board GGGVS
3073 to 3160 (m)	Any	Slip Alarm Inquiry Test (#144)	MIN/WRN**	OFF	test board GGGVS r 6
3585 to 3601 (o)	Any	Misframe Alarm Inquiry Test (#145)	MIN/WRN**	OFF	test board GGGVS r 6
3840(p)	Any	None			
3841(q)	4358				
3842(r)	46097				
3999(t)	Any	None			

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

**If ports are assigned to the Media Module, then a minor alarm is raised. If no ports are assigned to the Media Module, then a warning alarm is raised. The alarm is raised after the Media Module has been missing for a period of 15 minutes. Warning alarms are also raised against any ports administered on the Media Module.

***Minor alarms on this MO may be downgraded to warning alarms based on values set in the **set options** command.

Major alarms on this MO may be downgraded to minor or warning alarms based on values set in the **set options** command.

3 of 3

Notes:

- **(a) Error Type 1**— Indicates that the Media Module has totally stopped functioning or is not fully administered. The alarm is logged about 15 minutes after the Media Module has been removed or 11-minutes after the SAKI Test (#53) fails.To be fully administered, a MG-DS1 must meet all three of the following conditions:
  - Have an entry in the circuit plan using the **change media module** command
  - Be administered using the **add ds1 GGGVS** command
  - Be physically inserted into the correct slot

  If the Media Module has an entry in the circuit plan and either of the other two conditions are *not* met, a MINOR alarm is logged.

  1. To resolve the error do either of the following:
     - Make sure that all conditions for administration are met and that a functioning MG-DS1 is inserted in the correct slot.
     - Completely remove the MG-DS1 from the system using the following steps.
  2. Remove any administered DS1 trunks, access endpoints or PRI endpoints associated with the Media Module from their trunk groups.
  3. Execute the **remove ds1 GGGVS** and **change media module GGGVS** commands.
- **(b) Error Type 18** — The MG-DS1 Interface Media Module has been busied out by a **busyout board GGGVS** command.
- **(c) Error Type 23** — The MG-DS1 Media Module is not completely administered. To be fully administered, the MG-DS1 Media Module must:
  - Have an entry in the circuit plan using the **change media module** command
  - Be administered using the **add ds1 GGGVS** command
  - Be physically inserted into the correct slot

  A DS1 (MG-DS1, DS1-BD) differs from most Media Modules in that inserting the Media Module into the switch is not enough to make the board usable. It must also be administered with the **add ds1** command.
- **(d) Error Type 125: No Aux Data** — An incorrect Media Module is inserted in the slot where the MG-DS1 Media Module is logically administered.

  To resolve this problem, either:
  - Remove the incorrect Media Module and insert the logically administered Media Module.
  - Use the **change circuit-pack** command to re-administer this slot to match the Media Module inserted.
- **(e) Error Type 257** — This error is associated with the Common Port Media Module Maintenance Test.

  Refer to XXX-BD (Common Port Media Module) Maintenance documentation for details.

- **(f) Error Type 513** — The MG-DS1 (MM710) has detected a transient hardware problem.

  The value in the Aux Data field indicates the type of hardware problem:

Aux Data	Problem
4352	External RAM failure
4353	Internal RAM failure
4355	Internal ROM failure

  If the board detects only one of these hardware problems, then the error will disappear when none of these faults are detected for 10 minutes. If the same Aux Data value is logged more than once in a 24 hour period, the Media Module should be replaced.

- **(g) Error Type 514** — This is a LAN External RAM Error.

  This error occurs when there is a hardware fault in the PPE external RAM. The RAM is used for message buffering to and from the Packet Bus. This error should not occur frequently. If it does (10 times within 30 minutes), the Media Module should be replaced.

- **(h) Error Type 769** — This is a transmit FIFO Underflow Error.

  This error occurs when the Media Module cannot find the end of frame bit when transmitting a frame to the Packet Bus. An alarm is raised if this error occurs three times within 10 minutes. Clear the alarm using the following commands: **busyout board GGGVS**, **reset board GGGVS**, **test board GGGVS long**, **release board GGGVS**. If the error recurs within 10 minutes, replace the Media Module.

- **(i) Error Type 770** — This is an Unable to Write LAN Translation RAM Error.

  This error occurs when a call is aborted because there are no available translation RAM locations for the call connection attempt. An alarm is raised if this error occurs two times within 10 minutes. Clear the alarm using the following commands: **busyout board GGGVS**, **reset board GGGVS**, **test board GGGVS long**, **release board GGGVS**. If the error recurs within 10 minutes, replace the Media Module.

- **(j) Error Types 1400, 1401** — This is an Echo Cancellation error.

  Echo Cancellation errors are logged when:

  - Error 1400 - Echo canceller function failed. The Echo Canceller Function Test, which is executed by firmware, failed.
  - Error 1401 - Echo canceller memory failed. The Echo Canceller Memory Test, which is executed by firmware, failed.

  Echo Cancellation is no longer being supplied by the board. Clear the alarm using the following commands: **busyout board GGGVS**, **test board GGGVS long**, **release board GGGVS**. If Test #1420 (Echo Canceler Test) fails, replace the Media Module.

- **(k) Error type 1537** — This is a LAN Bus Timeout Error.

  This error occurs when the Media Module transmits too many bytes on the LAN bus for a single frame. This condition may be caused by an on-board fault or by faulty data received on one of the Media Module's external ports. If any of the ports on this Media Module are alarmed, refer to the repair procedures for those maintenance objects.

  If the error occurs three times within 10 minutes, the board is isolated from the Packet Bus and the board alarmed. To clear the alarm and restore the board to the Packet Bus, use the commands **busyout board GGGVS**, **reset board GGGVS**, **test board GGGVS long**, **release board GGGVS**.

  If the problem persists, and there are no PKT-BUS alarms or port alarms, then replace the Media Module.

- **(l) Error Type 1538** — The hyperactive Media Module is out-of-service and may exhibit one or more of the following symptoms:

  - The common Media Module level tests such as Test #50 abort with error code 2000.
  - The tests run on the ports of this Media Module return a NO-BOARD result.
  - A busyout/release of the Media Module has no affect on test results.
  - A **list configuration** command shows that the Media Module and ports are properly installed.

  The Media Module is isolated from the system and all trunks or ports on this Media Module are placed into the out-of-service state. The system will try to restore the Media Module within 20-30 minutes. When no faults are detected for 20-30 minutes, the MG-DS1 is restored to normal operation. All trunks or ports of the MG-DS1 are then returned to the in-service state.

  If the board is not restored to normal operation, or the error recurs after the board was restored to normal operation, escalate the problem.

- **(m) Error Types 3073 to 3160** — Error Type 3073 shows that this board is receiving slips and the AUX Data "minus 3072" shows the last slip count reported.

- **(o) Error Types 3585 to 3601** — Error Type 3585 shows that this board is receiving misframes, and the AUX Data "minus 3584" shows the last misframe count reported.

- **(p) Error Type 3840** — This error type is not service-affecting. No action is required.

  These errors are reported by the Media Module when it receives a bad control channel message from the switch. The auxiliary data identifies the following error events:

Aux Data	Event
4096	Bad major heading
4097	Bad port number
4098	Bad data
4099	Bad sub-qualifier

Aux Data	Event
4100	State inconsistency
4101	Bad logical link

- **(q) Error Type 3841**— The MG-DS1 (MM710) has detected a transient hardware logic error (for example, program logic inconsistency).

  This error will disappear when no faults are detected for 100 minutes.

- **(r) Error Type 3842** — This is a Bad Translation RAM Location Found Error.

  This error is not service-affecting. No action is required. A Bad Translation RAM is detected, but the call continues by using another translation location.

- **(t) Error Type 3999** — This error indicates that the Media Module sent a large number of control channel messages to the switch within a short period of time.

  If Error Type 1538 is also present, then the Media Module was taken out-of-service due to hyperactivity. If Error Type 1538 is not present, then the Media Module has not been taken out-of-service, but it has generated 50% of the messages necessary to be considered hyperactive. This may be completely normal during heavy traffic periods. However, if this error type is logged when the Media Module is being lightly used, it may indicate a problem with the Media Module or the equipment attached to it.

System Technician-Demanded Tests: Descriptions and Error Codes

Investigate tests in the order they are presented in Table 106: Technician-Demanded Tests on page 204. By clearing error codes associated with the Echo Cancellation Test, for example, you may also clear errors generated from other tests in the testing sequence.

Table 106: Technician-Demanded Tests *1 of 2*

Order of Investigation	Short Test Sequence	Long Test Sequence	Reset Board Sequence	test ds1-loop	D/ND*
Echo Cancellation Test (#1420)		X			D
Control Channel Loop Test (#52)		X			ND

1 of 2

Table 106: Technician-Demanded Tests *2 of 2*

Order of Investigation	Short Test Sequence	Long Test Sequence	Reset Board Sequence	test ds1-loop	D/ND*
NPE Connection Audit Test (#50) **NOTE:** This test will ABORT with Error Code 1412					
Loss of Signal Alarm Inquiry Test (#138)	X	X			ND
Blue Alarm Inquiry Test (#139)	X	X			ND
Red Alarm Inquiry Test (#140)	X	X			ND
Yellow Alarm Inquiry Test (#141)	X	X			ND
Major Alarm Inquiry Test (#142)	X	X			ND
Minor Alarm Inquiry Test (#143)	X	X			ND
Slip Alarm Inquiry Test (#144)	X	X			ND
Misframe Alarm Inquiry Test (#145)	X	X			ND
Translation Update Test (#146)	X	X			ND
SAKI Sanity Test (#53)			X		D
Internal Looparound Test (#135) **Note:** This test will ABORT with Error Code 1412			X		D

*D = Destructive; ND = Nondestructive

2 of 2

Control Channel Looparound Test (#52)

This test queries the Media Module for its Media Module vintage to verify angel communication.

Table 107: Test #52 Control Channel Looparound Test

Error Code	Test Result	Description/ Recommendation
None 2100	ABORT	System resources required for this test are not available. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	The Media Module failed to return the Media Module code or vintage. Retry the command a maximum of 5 times. If the problem continues, replace the Media Module. Retry the command a few times a maximum of 5 times.
	PASS	Communication with this Media Module is successful.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

SAKI Sanity Test (#53)

CAUTION:

This test resets the Media Module. The test is highly destructive and can only be initiated by a system technician-demanded **reset board GGGVS** command.

Table 108: Test #53 SAKI Sanity Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
None	ABORT	System resources required for this test are not available. Retry the **reset board** command at 1-minute intervals a maximum of 5 times.
1005	ABORT	Wrong Media Module configuration to run this test. This error applies only to DS1 Interface Media Modules. It means the DS1 Interface Media Module is providing timing for the system, and therefore, it cannot be reset without major system disruptions. If the Media Module needs to be reset, then set synchronization to another DS1 Interface Media Module or to the Tone-Clock Media Module and try again.
1015	ABORT	Port is not out-of-service. Busyout the Media Module. Execute the **reset board** command again.
2100	ABORT	System resources required for this test are not available. Retry the **reset board** command at 1-minute intervals a maximum of 5 times.
1	FAIL	The Media Module failed to reset.
2	FAIL	The Media Module failed to restart. Execute the **reset board** command again. If the problem persists, replace the Media Module.

1 of 2

Table 108: Test #53 SAKI Sanity Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
	PASS	The Media Module initializes correctly. Run the Short Test Sequence.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

Loss of Signal Alarm Inquiry Test (#138)

This test verifies the synchronization status, echo cancellation, and continuity of the DS1 link. The Loss of Signal alarm indicates that the MM710 Interface Media Module is unable to derive the synchronization clock from the DS1 facility. When the MM710 Interface Media Module detects a Loss of Signal alarm, it stops providing the synchronization clock for the system, if it is administered as a timing source, and transmits a Yellow alarm to the remote DS1 endpoint.

Note:

Synchronization is not administered from the SAT. It is administered via a CLI session with the G350 Media Gateway Processor.

When the Loss of Signal alarm is confirmed, maintenance software places all trunks or ports of the MM710 Interface Media Module into the out-of-service state. The inquiry test will run every 10 minutes until the loss of signal has been restored.

The MM710 Interface Media Module raises a Loss of Signal alarm after the signal has been lost for about 1 second. It will not retire the alarm until the signal has returned for about 10 seconds.

Echo Cancellation

If the MM710 firmware detects a serious echo canceller hardware error, it notifies maintenance software. When the maintenance subsystem receives notification of the echo cancellation error, it executes this *Loss Of Signal Alarm Inquiry* test.

This test, in addition to querying for a loss of signal condition and CSU errors, also queries MM710 to confirm the echo canceller error. A minor alarm is raised if the error is confirmed. The trunks of the board remain in-service since the board is still functional except for the echo cancellation capability.

If a loss of signal condition co-exists with CSU and/or echo canceller errors, the loss of signal condition takes priority, and the board and all trunks on the board are put in the out-of-service state. Errors are logged, however, for each error type.

When the maintenance subsystem receives notification that the echo canceller hardware error condition no longer exists, the maintenance subsystem restores the board and all trunks to their previous service state, if the alarm can be cleared (no other CSU errors or loss of signal conditions exist).

Note:

The DSU functionality is not available in this release of Communication Manager.

Table 109: TEST #138 Loss of Signal Alarm Inquiry Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 3

Table 109: TEST #138 Loss of Signal Alarm Inquiry Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 (MM710) interface Media Module is restored to normal operation. All of the trunks for the Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	MG-DS1 detects a Loss of Signal alarm. The physical link is broken or the remote DS1 endpoint is down. All trunks or ports of this MM710 are out-of-service. If the MG-DS1 connects to a T1 network facility: If the MM710 connects to a T1 facility, call the vendor of the T1 carrier to diagnose the remote DS1 endpoint. If the MM710 Interface Media Module connects directly to a switch, call the system technician of the remote switch to diagnose the DS1 endpoint. If the MG-DS1 connects to a line-side terminating device such as a PRI terminal adapter: Contact the vendor of the line-side terminating device to diagnose the equipment. Check the physical connection of the MM710 Interface Media Module and the cable. Check the physical connection of the MM710 Interface Media Module to the terminating device. Check premise distribution system (or intra-premise wiring) for physical connection failures.

2 of 3

Table 109: TEST #138 Loss of Signal Alarm Inquiry Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
1400	FAIL	Echo Canceller Function failed, this could be a hardware problem on the MM710: Use the **busyout board** command. Use the **test board long** command. Use the **release board** command. If Test 1420 still fails, replace the board.
1401	FAIL	Echo Canceller Function failed, this could be a hardware problem on the MM710: Use the **busyout board** command. Use the **reset board** command. Use the **test board long** command. Use the **release busy board** command. If the test still fails replace the board.
	PASS	DS1 signal is present and the physical link is healthy.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

3 of 3

Blue Alarm Inquiry Test (#139)

The Blue Alarm is a signal sent by the remote DS1 endpoint when it is out-of-service. The Blue Alarm Inquiry Test checks the blue alarm status of the remote DS1 endpoint.

When the MG-DS1 Interface Media Module detects a Blue Alarm signal from the remote DS1 endpoint, the Media Module transmits a Yellow alarm to the remote DS1 endpoint and sends a BLUE ALARM message to the maintenance software. When the Blue alarm is confirmed, the maintenance software places all trunks or ports of the MG-DS1 Interface Media Module into the out-of-service state. The inquiry test runs every 10 minutes until the Blue alarm is cleared.

The MG-DS1 Interface Media Module takes one second to recognize and report a Blue alarm and 16 seconds to recognize and report the resolution of a Blue alarm. When the Blue alarm is cleared, the MG-DS1 Interface Media Module stops transmitting the Yellow alarm and places the trunks or ports back into the service state before the Blue alarm occurs.

Line Loopback Alarm

The Line Loopback (LLB) is used by the remote DS1 endpoint to put the DS1 board into a loopback mode. When the DS1 board is in the LLB mode, the arriving bit pattern is regenerated and sent back. The Line Loopback (LLB) Alarm activates when the in-band activate LLB bit pattern arrives continuously for 5 seconds on the DS1 line. The LLB deactivates when the in-band deactivate LLB bit pattern arrives continuously for 5 seconds on the DS1 line.

Since LLB is a maintenance condition rendering all DS0 channels unavailable for signaling or bearer traffic, maintenance software treats this the same as a Blue Alarm.

Payload Loopback Alarm

The Payload Loopback (PLB) is used by the remote DS1 endpoint to put the switch DS1 into a loopback mode. The PLB Alarm activates when a network protocol activate bit pattern arrives over the 4Kbps ESF data link on the DS1 line. The PLB deactivates when a network protocol deactivate bit pattern arrives over the 4Kbps ESF data link on the DS1 line.

Since PLB is a maintenance condition rendering all DS0 channels unavailable for signaling or bearer traffic, maintenance software treats this the same as a Blue Alarm

Table 110: TEST #139 Blue Alarm Inquiry Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 3

Table 110: TEST #139 Blue Alarm Inquiry Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	The remote DS1 endpoint is out-of-service.
1 1794	FAIL	The MG-DS1 Interface Media Module detects a Line Loopback Alarm (LLB). If the DS1-M interface Media Module connects to a T1 facility, call the vendor of the T1 carrier to diagnose the remote DS1 endpoint. If the MG-DS1 interface Media Module connects directly to a switch, call the system technician of the remote switch to diagnose the DS1 endpoint. If the MG-DS1 interface Media Module connects directly to a line-side terminating device (for example, a PRI terminal adapter), call the vendor of the terminating device to diagnose the equipment.

2 of 3

Table 110: TEST #139 Blue Alarm Inquiry Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
1795	FAIL	The MG-DS1 Interface Media Module detects a Payload Loopback Alarm (PLB). If the MG-DS1 Interface Media Module connects to a leased T1 facility, call the vendor of the T1 carrier to diagnose the remote DS1 endpoint. If the MG-DS1 Interface Media Module connects directly to another DS1 board, call the system technician of the remote switch to diagnose the DS1 endpoint. If the MG-DS1 Interface Media Module connects directly to a line-side terminating device such as a PRI terminal adapter contact the vendor of the terminating device to diagnose the equipment.
	PASS	Remote DS1 endpoint is in-service. Neither a Blue alarm nor a Line Loopback alarm nor a Payload Loopback Alarm is detected by the MG-DS1 Interface Media Module.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MM-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

3 of 3

Red Alarm Inquiry Test (#140)

A MG-DS1 Interface Media Module raises a Red alarm when the framing pattern of the incoming DS1 bit stream has been lost. The Red Alarm Inquiry Test checks the framing status of a MG-DS1 Interface Media Module. A MG-DS1 Interface Media Module takes 3 seconds to recognize and report a Red alarm and 10 seconds to recognize and report the resolution of a Red alarm.

When the MG-DS1 Interface Media Module detects a Red alarm, the Media Module transmits a Yellow alarm to the remote DS1 endpoint and sends a RED ALARM message to the maintenance software. After the Red alarm is confirmed, the maintenance software places all trunks or ports of the Media Module into the out-of-service state. The inquiry test runs every 10 minutes until the Red alarm is cleared.

When the Red alarm is cleared, the MG-DS1 Interface Media Module stops transmitting the Yellow alarm to the remote DS1 endpoint. The maintenance software restores all trunks or ports of the MG-DS1 Interface Media Module to the service state it was in before the Red alarm occurred.

Loss of Multiframe Alarm

If the MG-DS1 Interface Media Module is administered using DMI-BOS signaling, the MG-DS1 Interface Media Module raises a Loss of Multiframe Alarm (LMA) when it cannot interpret the incoming signaling bits to synchronize to the multiframe pattern received in the 24th channel. Once the MG-DS1 Interface Media Module detects an LMA, the Media Module transmits a Remote Multiframe Alarm (RMA) to the remote DS1 endpoint. Maintenance software handles both Red alarm and LMA alarm(s) using the same mechanism.

Table 111: TEST #140 Red Alarm Inquiry Test *1 of 4*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.

1 of 4

Table 111: TEST #140 Red Alarm Inquiry Test *2 of 4*

Error Code	Test Result	Description/ Recommendation
	FAIL	The MG-DS1 interface Media Module detected a red alarm. An out of frame condition occurred on the MG-DS1 interface Media Module. The MG-DS1 interface Media Module will transmit a yellow alarm to the remote MG-DS1 endpoint until the red alarm is retired. If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 2. Contact T1 Network Service or a technician at the far-end switch to diagnose the remote DS1 endpoint. 3. Check the physical connectivity of the MG-DS1 packs and of the cable. 4. Replace the local MG-DS1 interface Media Module, and repeat the test. If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 5. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 6. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 7. Contact the vendor of the line-side terminating device to diagnose the equipment. 8. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 9. Replace the local MG-DS1 interface Media Module and repeat the test.

2 of 4

Table 111: TEST #140 Red Alarm Inquiry Test *3 of 4*

Error Code	Test Result	Description/ Recommendation
1	FAIL	The test failed. The MG-DS1 interface Media Module detected a loss of multiframe alarm (LMA). An out of frame condition occurred on the MG-DS1 interface Media Module. The MG-DS1 interface Media Module will transmit a remote multiframe alarm (RMA) to the remote MG-DS1 endpoint until the LMA is retired. If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 2. Contact T1 Network Service or a technician at the far-end switch to diagnose the remote DS1 endpoint. 3. Check the physical connectivity of the MG-DS1 packs and of the cable. 4. Replace the local MG-DS1 interface Media Module, and repeat the test. If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 1. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 2. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 3. Contact the vendor of the line-side terminating device to diagnose the equipment. 4. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 5. Replace the local MG-DS1 interface Media Module and repeat the test.

3 of 4

Table 111: TEST #140 Red Alarm Inquiry Test *4 of 4*

Error Code	Test Result	Description/ Recommendation
	PASS	No Red alarm is detected on the MG-DS1 Interface Media Module.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.
		4 of 4

Yellow Alarm Inquiry Test (#141)

Receiving a Yellow alarm from a remote DS1 endpoint indicates that the remote DS1 endpoint has an out-of-frame condition. The Yellow Alarm Inquiry Test is used to determine whether the remote DS1 endpoint is transmitting a Yellow alarm. The MG-DS1 Interface Media Module takes 500 msec to recognize and report a Yellow alarm and 500 msec to recognize and report that a Yellow alarm condition is cleared.

When the MM-DS1 Interface Media Module detects a Yellow alarm from the remote DS1 endpoint, it sends a YELLOW-ALARM uplink message to the maintenance software. After the maintenance software receives the YELLOW-ALARM message, the Yellow Alarm Inquiry Test is run to confirm the Yellow alarm. Once the Yellow alarm is confirmed, the maintenance software places all trunks or ports on the Media Module into the out-of-service state. The Inquiry Test runs every 10 minutes until the Yellow alarm is cleared.

When the Yellow alarm is cleared, the maintenance software restores all trunks or ports on the MG-DS1 Interface Media Module back to their previous service state before the Yellow alarm was raised.

This Yellow alarm corresponds to the yellow F2 state documented in CCITT Recommendation I.431.

Remote Multiframe Alarm

Remote Multiframe Alarm (RMA) indicates that the remote DS1 endpoint is in a Loss of Multiframe Alarm condition while the MG-DS1 Interface Media Module is administered using the DMI-BOS common channel signaling. The RMA is handled as a Yellow alarm.

Yellow F5 Fault Alarm

For 32-channel E1 operation with CRC4 on, the F5 fault state is defined as a fault in the user-network interface, specifically in the direction from the user (PBX) to the network. Refer to CCITT recommendation I.431.

Table 112: TEST #141 Yellow Alarm Inquiry Test *1 of 5*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.

1 of 5

Table 112: TEST #141 Yellow Alarm Inquiry Test *2 of 5*

Error Code	Test Result	Description/ Recommendation
	FAIL	The MG-DS1 interface Media Module detected a yellow alarm sent by the remote DS1 endpoint. An out of frame condition occurred at the DS1 endpoint. If the MM-DS1 connects to a T1 network facility or to another switch, do the following: 1. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 2. Contact T1 Network Service or a technician at the far-end switch to diagnose the remote DS1 endpoint. 3. Check the physical connectivity of the MG-DS1 packs and of the cable. 4. Replace the local MG-DS1 interface Media Module, and repeat the test. If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 1. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 2. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 3. Contact the vendor of the line-side terminating device to diagnose the equipment. 4. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 5. Replace the local MG-DS1 interface Media Module and repeat the test.

2 of 5

Table 112: TEST #141 Yellow Alarm Inquiry Test *3 of 5*

Error Code	Test Result	Description/ Recommendation
1	FAIL	The MG-DS1 interface Media Module detected a remote multiframe alarm (RMA) sent by the remote DS1 endpoint. An out of frame condition occurred at the DS1 endpoint. If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 2. Contact T1 Network Service or a technician at the far-end switch to diagnose the remote DS1 endpoint. 3. Check the physical connectivity of the MG-DS1 packs and of the cable. 4. Replace the local MG-DS1 interface Media Module, and repeat the test. If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 1. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 2. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 3. Contact the vendor of the line-side terminating device to diagnose the equipment. 4. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 5. Replace the local MG-DS1 interface Media Module and repeat the test.

3 of 5

Table 112: TEST #141 Yellow Alarm Inquiry Test *4 of 5*

Error Code	Test Result	Description/ Recommendation
2	FAIL	The MG-DS1 interface Media Module is reporting a Yellow F5 fault alarm. There is a fault in the User-Network interface from the user (PBX) to the network. An out-of-frame condition occurs on the remote DS1 endpoint. If the MG-DS1 connects to a T1 network facility: 1. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 2. Contact T1 Network Service to diagnose the remote DS1 endpoint. 3. Check the physical connectivity of the DS1 Interface Media Modules and cable. 4. Replace the local MG-DS1 Interface Media Module and repeat the test. If the MG-DS1 connects to a line-side terminating device such as a PRI terminal adapter: 1. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 2. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 3. Contact the vendor of the line-side terminating device to diagnose the equipment. 4. Check the physical connection of the MG-DS1 Interface Media Module to the terminating device. Check premise distribution system (or intra-premise wiring) for physical connection failures. 5. Replace the local MG-DS1 Interface Media Module and repeat the test.

4 of 5

Table 112: TEST #141 Yellow Alarm Inquiry Test *5 of 5*

Error Code	Test Result	Description/ Recommendation
	PASS	Neither a Yellow alarm nor a Remote Multiframe Alarm nor a F5 state alarm is being received from the remote DS1 endpoint.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

5 of 5

Major Alarm Inquiry Test (#142)

The Major alarm raised by a MG-DS1 Interface Media Module indicates that the average bit error rate on the DS1 facility is greater than 1/1000. The Major Alarm Inquiry Test is used to determine that the received DS1 bit error rate is greater than 1/1000. The MG-DS1 Interface Media Module takes 10 seconds to recognize and report a Major alarm and 10 seconds to recognize and report that a Major alarm condition is cleared.

When the MG-DS1 Interface Media Module detects a Major alarm, it sends a MAJOR-ALARM message to the maintenance software. (32-channel interfaces send a YELLOW alarm to the far end). After the maintenance software receives a MAJOR-ALARM message, the Major Alarm Inquiry Test is initiated to confirm the Major alarm on the MG-DS1 Interface Media Module. The Inquiry Test runs every 10 minutes until the Major alarm is cleared. The maintenance software places all trunks or ports on the Media Module in the out-of-service state if the Major alarm persists for more than 20 minutes.

When the Major alarm is cleared, the maintenance software restores all trunks or ports on the Media Module to their previous service state before a Major alarm occurs.

Table 113: TEST #142 Major Alarm Inquiry Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 3

Table 113: TEST #142 Major Alarm Inquiry Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
	FAIL	If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. The performance of the DS1 link between the MG-DS1 interface Media Module and the remote DS1 endpoint is very poor. Enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 2. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 3. Contact T1 Network Service or the technician at the remote switch to diagnose the equipment. 4. Check the physical connectivity of the MG-DS1 interface Media Modules and the cable. 5. Replace the local MG-DS1 interface Media Module, and repeat the test.
	FAIL *(cont'd.)*	If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 1. The performance of the DS1 link between the MG-DS1 interface Media Module and the line-side terminating device is very poor. Enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 2. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 3. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 4. Contact the vendor of the line-side terminating device to diagnose the equipment. 5. Check the physical connection of the MG-DS11 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 6. Replace the local MG-DS1 interface Media Module and repeat the test.

Table 113: TEST #142 Major Alarm Inquiry Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
	PASS	No Major alarm is detected in the MG-DS1 Interface Media Module.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MM-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.
		3 of 3

Minor Alarm Inquiry Test (#143)

The Minor alarm raised by a MG-DS1 Interface Media Module indicates that the average bit error rate on the DS1 facility is greater than 1/1,000,000, but less than 1/1000. The Minor Alarm Inquiry Test is used to determine that the received DS1 bit error rate is greater than 1/1,000,000 and less than 1/1000. When D4 framing mode is selected, the MG-DS1 Interface Media Module takes 41-minutes to recognize and report a Minor alarm and 41-minutes to recognize and report that a Minor alarm condition has cleared. If ESF framing mode is selected, the MG-DS1 Interface Media Module takes 10 minutes to recognize and report a Minor alarm and 10 minutes to recognize and report that a Minor alarm condition has cleared.

When the MG-DS1 Interface Media Module detects a Minor alarm condition, it sends a MINOR-ALARM message to the maintenance software. After the maintenance software receives a MINOR-ALARM message, the Minor Alarm Inquiry Test is initiated to confirm the Minor alarm. All trunks or ports on the Media Module are kept in the in-service state after the Minor alarm is confirmed. The Minor Alarm Inquiry Test runs every 10 minutes until the Minor alarm is cleared.

Table 114: TEST #143 Minor Alarm Inquiry Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 3

Table 114: TEST #143 Minor Alarm Inquiry Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
	FAIL	Minor alarms are often accompanied by slip and misframe alarms against the board. Trunk alarms and hardware error logs may occur on the associated trunks. If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. The performance of the DS1 link between the MG-DS1 interface Media Module and the remote DS1 endpoint is poor. Enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 2. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 3. Contact T1 Network Service or the technician at the remote switch to diagnose the equipment. 4. Check the physical connectivity of the MG-DS1 interface Media Modules and the cable. 5. Replace the local MG-DS1 interface Media Module, and repeat the test.

2 of 3

Table 114: TEST #143 Minor Alarm Inquiry Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
	FAIL *(cont'd.)*	If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 1. The performance of the DS1 link between the MG-DS1 interface Media Module and the line-side terminating device is very poor. Enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 2. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 3. Investigate the maintenance status of the line-side terminating device. Obtain the error seconds measurement on the terminating device (if possible). Refer to the 'Line-Side Terminating Device Operating Manual' for information. 4. Contact the vendor of the line-side terminating device to diagnose the equipment. 5. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 6. Replace the local MG-DS1 interface Media Module and repeat the test.
	PASS	No Minor alarm is detected in the MG-DS1 Interface Media Module.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

3 of 3

Slip Alarm Inquiry Test (#144)

Slips occur when transmitter and receiver are not running at precisely the same clock rate. The MG-DS1 Interface Media Module can detect both positive and negative slips on the DS1 facility. The Slip Alarm Inquiry Test is used to acquire the total number of slips that have occurred on a DS1 link.

When the MG-DS1 Interface Media Module detects a slip condition, the Media Module increments the on-board slip counter by one. A SLIP-COUNT message is spontaneously sent to the system software after the counter reaches a threshold (for example, 88). When the maintenance software receives the SLIP-COUNT message, the Slip Alarm Inquiry Test is initiated to query the slip counters on a MG-DS1 Interface Media Module and total the slip counts in the maintenance software.

If the count of slips is over the threshold, a Minor alarm is raised against the MG-DS1 Interface Media Module. All trunks or ports of the MG-DS1 Interface Media Module remain in the in-service state.

Table 115: TEST #144 Slip Alarm Inquiry Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.

1 of 3

Table 115: TEST #144 Slip Alarm Inquiry Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
1 to 88	FAIL	The test failed because the MG-DS1 interface Media Module and the remote DS1 endpoint are not synchronized to the same clock rate. The MG-DS1 interface Media Module detected a slip alarm. The error code equals the number of slips detected by the MG-DS1 interface Media Module since the last slip alarm inquiry test. If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. Retry the command at 1-minute intervals for a maximum of 5 times. 2. For a DS1 interface Media Module, enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 3. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 4. Contact T1 Network Service or the technician at the remote switch to diagnose the remote DS1 endpoint. 5. Check the physical connectivity of the MG-DS1 interface Media Modules and the cable. 6. Replace the local MG-DS1 interface Media Module, and repeat the test.

2 of 3

Table 115: TEST #144 Slip Alarm Inquiry Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
1 to 88 *(cont.)*	FAIL *(cont'd.)*	If the MG-DS1 connects to a line-side terminating device (for example, a PRI terminal adapter), do the following: 1. Retry the command at 1-minute intervals for a maximum of 5 times. 2. Enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 3. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 4. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 5. Contact the vendor of the line-side terminating device to diagnose the equipment. 6. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 7. Replace the local MG-DS1 interface Media Module and repeat the test.
	PASS	No Slip alarm is detected on the MG-DS1 Interface Media Module.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

3 of 3

Misframe Alarm Inquiry Test (#145)

Misframe Alarm indicates that framing bits observed on a MG-DS1 Interface Media Module are in error. The Misframe Alarm Inquiry Test queries the total number of misframes that have occurred on a DS1 Interface Media Module since the last inquiry.

When the DS1 Interface Media Module detects a misframe error, it increments its misframe counter by one. If the counter reaches a specified threshold (i.e., 17), a MISFRAME-COUNT message is automatically sent to the switch maintenance software. After the maintenance software receives the MISFRAME-COUNT message, the Misframe Alarm Inquiry Test is initiated to collect the misframe counts from the MG-DS1 Interface Media Module.

A Minor alarm against the MG-DS1 Interface Media Module is raised, but all trunks or ports of the MG-DS1 Interface Media Module remain in the in-service state.

Table 116: TEST #145 Misframe Alarm Inquiry Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.

1 of 3

Table 116: TEST #145 Misframe Alarm Inquiry Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
1 to 17	FAIL	The test failed because the MM-DS1 interface Media Module detected errors in the received framing bits pattern. The error code equals the number of misframes detected by the MG-DS1 interface Media Module since the last misframe alarm inquiry test. Major bit and minor bit error rate (error types 2561 and 2817) error logs often accompany misframe alarms. Clearing the cause of these error logs may clear the misframes which are occurring. If the MG-DS1 connects to a T1 network facility or to another switch, do the following: 1. Retry the command at 1-minute intervals for a maximum of 5 times. 2. If the DS1 interface Media Module is a MM710, enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 3. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. 4. Contact T1 Network Service or the technician at the remote switch to diagnose the remote DS1 endpoint. 5. Check the physical connectivity of the MG-DS1 interface Media Modules and the cable. 6. Replace the local MG-DS1 interface Media Module, and repeat the test.

2 of 3

Table 116: TEST #145 Misframe Alarm Inquiry Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
1 to 17 *(cont.)*	FAIL *(cont'd.)*	If the MM-DS1 connects to a line-side terminating device such as a PRI terminal adapter: 1. Retry the command at 1-minute intervals for a maximum of 5 times. 2. Enter the **list measurement ds1-log GGGVS** command to read the error seconds measurement. 3. Verify that the switch DS1 and the line-side terminating device are administered using the same signaling mode, framing mode, and line coding. 4. Investigate the maintenance status of the line-side terminating device. Refer to the 'Line-Side Terminating Device Operating Manual' for information. 5. Contact the vendor of the line-side terminating device to diagnose the equipment. 6. Check the physical connection of the MG-DS1 interface Media Module to the terminating device, and check the premise distribution system (or the intra-premise wiring) for physical connection failures. 7. Replace the local MG-DS1 interface Media Module and repeat the test.
	PASS	No Misframe alarm is detected on the MM-DS1 Interface Media Module.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MM-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

3 of 3

Translation Update Test (#146)

The Translation Update Test sends the circuit-pack-level information specified by System Administration to the MG-DS1 Interface Media Module. Translation includes the following data administered for a MG-DS1 Interface Media Module (see output of **display ds1 GGGVS** command): DS1 Link Length between two DS1 endpoints, Synchronization Source Control, All Zero Suppression, Framing Mode, Signaling Mode, Time Slot Number of 697-Hz Tone, Time Slot Number of 700-Hz Tone, etc.

Table 117: TEST #146 Translation Update Test

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Internal system software error. Enter the **display ds1 GGGVS** command to verify the DS1-MM Interface Media Module translation.
	PASS	Translation data has been downloaded to the DS1-M Interface Media Module successfully.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

Echo Canceller Test (#1420)

CAUTION:

This test is executed only for MM710 Media Modules that have been administered on the DS1 Media Module form to provide echo cancellation. The MM710 must be busied out before this demand test is run.

CAUTION:

This test is for the MM710 Media Module. The test originates from a manually initiated **test board long** demand test of a TMM710 Media Module. The test instructs firmware to test the echo cancellation circuity. The MM710 firmware tests echo cancellation on a subset of channels. If any channel fails twice, or if any two channels fail once, the test fails, and echo cancellation is bypassed on all channels of the board. Otherwise the test passes, and echo cancellation is configured to the administered parameters.

Table 118: Test #1420 Echo Canceller Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
1015	ABORT	The board is not busied out. This test will abort if the MG-DS1 Media Module under test is in service.
2000	ABORT	Response to the test was not received within the allowable time period. This may be due to hyperactivity. Error Type 1538 in the error log indicates hyperactivity. The hyperactive Media Module is out of service and one or more of the following symptoms may be exhibited. The MG-DS1 tests (such as Test #138 and Test #139) are aborting with error code 2000. The tests run on the ports of this Media Module are returning a no board result. A **busyout** or a **release** command has no affect on the test results. A **list config** command shows that the Media Module and the ports are properly installed. When hyperactivity occurs, the Media Module is isolated from the system, and all of the trunks for this Media Module are placed into the out of service state. The system will try to restore the Media Module within 15 minutes. When no faults are detected for 15 minutes, the MG-DS1 interface Media Module is restored to normal operation. All of the trunks for the MG-DS1 interface Media Module are then returned to the in service state. Hyperactivity is often caused by the associated facility. In such a case, faults (such as slips, misframes, or blue alarms) would be entered in the error log. In addition, many hardware errors would be logged against the associated trunk circuits. If the facility is OK and the error occurs again after 15 minutes, replace the Media Module.

1 of 2

Table 118: Test #1420 Echo Canceller Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
2012	ABORT	Internal system error. Retry the command at 1-minute intervals for a maximum of 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
2500	ABORT	Internal system error. Retry the command at 1-minute intervals for a maximum of 5 times.
1400, 1401	FAIL	The Echo Cancellation Test has failed: Error 1400 - Echo canceller function failed. The Echo Canceller Function Test, which is executed by firmware, failed. Error 1401 - Echo canceller memory failed. The Echo Canceller Memory Test, which is executed by firmware, failed. Echo Cancellation is no longer being supplied by the board. Clear the alarm using the following commands: **busyout board GGGVS**, **test board GGVS long**, **release board GGVS**. If the test still fails, replace the Media Module. When this test fails, echo cancellation will be bypassed on all channels on the board. The Media Module can still be used for a T1/E1 line interface without echo cancellation. This capability provides limited service for the customer until the Media Module can be changed out.
	PASS	The Echo Cancellation feature is functioning properly.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MM-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

MG-ICC (Internal Call Controller)

Table 119: MG-ICC (Internal Call Controller)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
MG-ICC	MAJOR	None	INTERNAL CALL CONTROLLER
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			

This maintenance object monitors the H.323 link between the S8300 Media Server running as an LSP and the primary call controller. It logs errors when the keep alive messages that are exchanged between the servers fail. These messages indicate the status of the H.323 link between the two. If the keep alive messages are active all is well; if not, an error is logged.

Error log entry and test to clear value

Table 120: MG-ICC error log entries

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
1(a)		None	MAJOR	OFF	

Notes:

- **(a) Error Type 1**: this error type indicates a failure of the H.323 link keep alive messages between the LSP and primary call controller. This is an indication that the LAN or the primary call controller is down.

System Technician-Demanded Tests: Descriptions and Error Codes

There are no System Technician-Demanded Tests associated with this MO.

PLAT-ALM (Platform Alarms)

The PLAT_ALM is a virtual MO used by Communication Manager to keep track of Media Server alarms. A MAJOR, MINOR, or WARNING alarm can be logged against this MO to indicate the presence of one or more Media Server alarms.

A technician who is using the SAT and finds an alarm against the PLAT-ALM MO must:

1. Log into the Media Server's Web interface.
2. To see the Media Server's current list of alarms, select the **Display Alarms** option.
3. To troubleshoot and clear the problems, follow the procedures for the appropriate MOs listed in the display.

   Note:

   After repairing the Media Server, clear every Media Server alarm. This action will also clear any alarms associated with the PLAT-ALM MO.

System Technician-Demanded Tests: Descriptions and Error Codes

There are no System Technician-Demanded Tests associated with this MO.

TIE-DS1 (DS1 Tie Trunk)

Table 121: TIE-DS1 (DS1 TIE TRUNK)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run	Full Name of MO
TIE-DS1*	MAJOR**	test trunk *grp/mbr* l	DS1 Tie Trunk
TIE-DS1	MINOR	test trunk *grp/mbr* l	DS1 Tie Trunk
TIE-DS1	WARNING	test trunk *grp/mbr*	DS1 Tie Trunk
*See MG-DS1 documentation if the tie trunk is on a MM710 Media Module Media Module.			
A MAJOR alarm on a trunk indicates that alarms on these trunks are not downgraded by the **set options command and that at least 75% of the trunks in this trunk group are alarmed.			

Many trunk problems are caused by incorrect settings of parameters on the trunk group administration form. Settings must be compatible with the local environment and with parameter settings on the far-end. Refer to "*Administrator's Guide for Avaya Communication Manager*, 555-233-506" for information on how to administer trunks. For the correct settings for administrable timers and other parameters on a country-by-country basis, see your local Avaya representative.

The DS1 tie trunk provides both voice and data communications between two PBX switches. There are two types of DS1 interfaces:

- 24 DS0 channels on a 1.544 Mbps link
- 31 DS0 channels + 1 framing channel on a 2.048 Mbps link

DS1 Tie Trunks are used widely in the Distributed Communications System (DCS) and Central Attendant Service (CAS) system features.

A DS1 tie trunk can also be used as an access endpoint which is a non-signaling channel with bandwidth for voice-grade data, 56 Kbps data or 64 Kbps data.

DS1 tie trunk maintenance provides a strategy to maintain a DS1 tie trunk via a port on the MM710 Interface Media Modules.

The DS1 tie trunk maintenance strategy covers logging DS1 tie trunk hardware errors, running tests for trunk initialization, periodic and scheduled maintenance, system technician-demanded tests, and alarm escalation and resolution. Three different trunk service states are specified in DS1 tie trunk maintenance:

Out-of-service	The trunk is deactivated and cannot be used for incoming or outgoing calls.
In-service	The trunk is activated and can be used for both incoming and outgoing calls.
Disconnect (ready-for-service)	The trunk is in an activated state but can only be used for an incoming call.

If the DS1 Interface Media Module is out of service, then all trunks on the DS1 Interface Media Module are also placed into the out-of-service state and a Warning alarm is raised.

Hardware Error Log Entries and Test to Clear Values

Table 122: DS1 Tie Trunk Maintenance Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test trunk *grp*/*mbr*
1(a)	57476 57477 57485 57487				
15(b)	Any	Port Audit and Update Test (#36)			
18(c)	0	busyout trunk *grp*/*mbr*	WARNING	OFF	release trunk *grp*/*mbr**
19(d)	0	None			
130(e)		None	WARNING	ON	test trunk *grp*/*mbr*
257(f)	57473 57474				
513(g)	57392	DS1 Tie Trunk Seizure Test (#136)	MIN/MAJ		
769(h)	57393	DS1 Tie Trunk Seizure Test (#136)	MIN/MAJ		
1025		DS1 Tie Trunk Seizure (Test #136)	MIN/ WRN***	OFF	test trunk *grp*/*mbr* r 2
1793(i)					test board GGGVSpp long
2305(j)	50944	DS1 Tie Trunk Seizure Test (#136)	MIN/MAJ	OFF	
2562(k)	16665				
2817(l)	52992				
3840(m)	Any	Port Audit and Update (Test #36)			

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

1 of 2

Table 122: DS1 Tie Trunk Maintenance Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
***This alarm will only be raised when the System-Parameter Country form has the Base Tone Generator field set to 4 (Italy). This alarm will be a MINOR alarm unless 75% or more trunks in this trunk group are out of service, then the alarm will be upgraded to a MAJOR alarm.					
****Major or Minor alarms on this MO may be downgraded to Warning alarms based on the values used in the **set options** command.					
					2 of 2

Notes:

- (a) Error Type 1—The DS1 Interface Media Module detects a hardware error on the DS1 tie trunk. This error can be caused by incompatible translations. Make sure the parameters administered on the DS1 Media Module form match those administered on the far-end switch. See *Administrator's Guide for Avaya Communication Manager*, 555-233-506, for details.

  The Aux Data field indicates the following hardware error types:

57476	On-hook before wink
57477	On-hook before ready to receive digits
57485	Wink too short for valid signal
57487	The timer expired while waiting for an off-hook signal from the far end as a response at end of digits dialing. Check the far-end switch for related problems.

  If all administration errors between the switch and the far-end match, and these errors continue to recur, follow normal escalation procedures.

- (b) Error Type 15—This is a software audit error that does not indicate any hardware malfunction. Run Short Test Sequence and investigate associated errors (if any).
- (c) Error Type 18—The DS1 tie trunk has been busied out by a **busyout trunk** grp/mbr command. No calls can be made on this trunk except for the Facility Access Test Call. Facility Access Test Calls are described in Chapter 6 and in *Administrator's Guide for Avaya Communication Manager*, 555-233-506.
- (d) Error Type 19—This error type indicates that the far-end may be out-of-service, or the Electronic Tandem Network may be busied out.
- (e) Error Type 130—This error type indicates that the Media Module has been removed or has been insane for more than 11-minutes. To clear the error, reinsert or replace the Media Module.

- (f) Error Type 257—The DS1 Interface Media Module detects a hardware error on the DS1 tie trunk. The trunk cannot communicate with the far end because it is unable to interpret digits sent from the far-end switch. The Aux Data field indicates the following:

57473	The rotary dial rate is below 8 pulses per second.
57474	The rotary dial rate is above 12 pulses per second.

  Check with the far-end switch or operating company for proper trunk connection.

- (g) Error Type 513—DS1 Interface Media Module detects a hardware error on the DS1 tie trunk. The trunk is in-service/active and waiting for an “on-hook” from the far-end switch. No calls can be routed over the trunk while it is in this state. Aux Data 57392 indicates no external release on PBX disconnect. Check with the far-end switch or operating company for proper trunk connection.
- (h) Error Type 769—The DS1 Interface Media Module detects a hardware error on the DS1 tie trunk. This error usually occurs after an occurrence of error type 513. The trunk has received the belated “on-hook” that it has been waiting for from the far-end switch. The trunk is restored to in-service/idle and can be used for calls. Aux Data 57393 indicates delayed external release on PBX disconnect. This error can be ignored.
- (i) Error Type 1793—The DS1 Interface Media Module is out-of-service. See MG-DS1 Maintenance documentation for details.
- (j) Error Type 2305—Reorder message. The trunk could not be seized. This error causes the Trunk Seizure Test (#136) to run and is only a problem if the Seizure Test fails (in which case Error Type 1025 also appears). In this case, the trunk may be put in “Ready-for-Service” state (shown as “disconnected” by the status command), which allows only incoming calls. Run the Trunk Seizure Test (#136) and follow its procedures.
- (k) Error Type 2562—Retry Failure error. This error is logged only. It is not a hardware failure and hence does not start any testing or generate any alarms. This error comes from call processing and is generated when a second attempt (retry) to seize an outgoing trunk fails.
- (l) Error Type 2817—Glare error. This error is logged only. It is not a hardware failure and hence does not start any testing or generate any alarms. This error is the result of a simultaneous seizure of a two-way trunk from both the near-end and the far-end. Attempt to place the call again. If the error persists, execute the DS1 Tie Trunk Seizure Test (#136) and follow its outlined procedures.
- (m) Error Type 3840—Port Audit and Update Test (#36) failed due to an internal system error. Enter **status trunk** command and verify the status of the trunk. If the trunk is out-of-service, then enter **release trunk** command to put it back to in-service. Retry the test command.

System Technician-Demanded Tests: Descriptions and Error Codes

Always investigate tests in the order presented in the table below when inspecting errors in the system. By clearing error codes associated with the *NPE Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 123: System Technician-Demanded Tests

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** *This Test will abort with Error Code 1412*		X	ND
Conference Circuit Test (#7) **Note:** *This Test will abort with Error Code 1412*		X	ND
DS1 Tie Trunk Seizure Test (#136)	X	X	ND
Port Audit and Update Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Port Audit and Update Test (#36)

This test sends port level translation data from switch processor to the DS1 Interface Media Module to ensure that the trunk's translation is correct. Translation updates include the following data: trunk type (in/out), dial type, timing parameters, and signaling bits enabled. The port audit operation verifies the consistency of the current state of the trunk kept by the DS1 Interface Media Module and the switch software.

Table 124: TEST #36 Audit and Update Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.

1 of 3

Table 124: TEST #36 Audit and Update Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
1000	ABORT	System resources required to run this test were not available. The port may be busy with a valid call. Use the **display port GGGVSpp** command to determine the trunk group/ member number of the port. Use the **status trunk** command to determine the service state of the port. If the service state indicates that the port is in use, then the port is unavailable for certain tests. You must wait until the port is idle before retesting. If the port status is active but the port is not in use (no calls), check the error log for error type 1025 (see the error log table for a description of this error and required actions). The port may be locked up. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1006	ABORT	The test was aborted because the trunk is out of service. Use the **status trunk** command to verify that the trunk is out of service. If the trunk is out of service, determine why. If it is OK to put the trunk back in service, use the **release trunk** command to put the trunk back in service, and then retry the test.
2000	ABORT	Response to the test request was not received within the allowable time period.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Internal system error. Retry the command at 1-minute intervals a maximum of 5 times.
	PASS	Trunk translation has been updated successfully. The current trunk states kept in the DS1 Interface Media Module and switch software are consistent. If the trunk is busied out, the test will not run but will return PASS. To verify that the trunk is in-service: Enter the **status trunk** command to verify that the trunk is in-service. If the trunk is in-service, no further action is necessary. If the trunk is out-of-service, continue to step 2. Enter the **release trunk** command to put the trunk back into in-service. Retry the test command.

2 of 3

Table 124: TEST #36 Audit and Update Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Check to ensure that the board translations are correct. Use the **list config** command, and resolve any problems that are found. If the board was found to be correctly inserted in step 1, use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port. If this is not the case, check to see that there is a valid board inserted.

3 of 3

DS1 Tie Trunk Seizure Test (#136)

The DS1 Tie Trunk Seizure Test is run to verify the trunk's signaling capability. The test is composed of two parts. The first part queries the Media Module for the following errors: Loss of Signal, Red Alarm, Blue Alarm, Yellow Alarm, and Hyperactivity Alarm. The second part of the test is performed by sending a seizure message to the DS1 Interface Media Module and expecting an active reply by the DS1 Interface Media Module. If maintenance software does not receive any reply and the timer expires, the test fails. Once the active message is received, a dial pause message is sent to the DS1 Interface Media Module. If the DS1 Interface Media Module replies with a dial pulse tone message when the far end responds to the seizure, then the DS1 tie trunk Seizure Test passes. If the far end does not respond to the seizure and the timer expires, and the DS1 Interface Media Module sends a reorder message back to the maintenance software, then the test fails.

This second part of this test *cannot* be run on a trunk if one of the following cases is true:

- The trunk direction is administered as an incoming only trunk.
- The trunk is the 24th port on a DS1 Interface Media Module which is administered using 24th Common Channel Signaling.
- The trunk has been seized by a normal trunk call.
- The trunk is administered with maintenance test disabled.
- The outgoing signal type of the trunk is either automatic or immediate-start.
- This test always passes if the associated board is the TN802 IP trunk Media Module.

Table 125: TEST #136 DS1 Tie Trunk Seizure Test *1 of 3*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
1000	ABORT	System resources required to run this test were not available. The port may be busy with a valid call. Use the **display port GGGVSpp** command to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. If the port status is active but the port is not in use (no calls), check the error log for error type 1025 (see the error log table for a description of this error and required actions). The port may be locked up. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1004	ABORT	Far end is seizing the trunk while the test is ongoing. A glare situation is detected. Current test is designed to be aborted. Use the **display port GGGVSpp** command to determine the trunk group/member number of the port. Use the **status trunk** command to determine the service state of the port. If the port is in use, wait until the port is idle before testing. If the port status is idle, retry the command at 1-minute intervals for a maximum of 5 times.
1005	ABORT	Test failed due to incompatible configuration administered in trunk group form. Verify the following fields on the trunk group administration screen: Is trunk direction incoming only? Is trunk outgoing type either automatic or immediate-start? Is trunk the 24th port of the DS1 Interface Media Module while common control channel signaling is specified? If the trunk has been administered using the above information, then this test should abort.
1018	ABORT	The test was disabled via translation. You may want to determine why the test has been disabled before you enable it. Verify that the ’Maintenance Test’ field on the ’Trunk Administration’ screen is set to ’n.’ To enable the test, change the trunk administration and enter ’y’ into the ’Maintenance Test’ field. Repeat the test.

1 of 3

Table 125: TEST #136 DS1 Tie Trunk Seizure Test *2 of 3*

Error Code	Test Result	Description/ Recommendation
1020	ABORT	The test did not run due to an already existing error on the specific port or due to a more general Media Module error. Examine the error log for existing errors against this port or the Media Module and attempt to diagnose the already existing error. Retry the test.
1040	ABORT	The test is invalid for this trunk port because it is administered as an access endpoint. Use **display port** to verify that this port is administered as an access endpoint. In this case the test should abort.
2000	ABORT	Response to the test request was not received within the allowable time period. Retry the command at 1-minute intervals for a maximum of 5 times.
2053	ABORT/ FAIL*	At least one of the following errors is found on the DS1 Media Module: 1281: Loss of Signal 1793: Blue Alarm 2049: Red Alarm 2305: Yellow Alarm 1537: Hyperactivity Look for the above error types in the Hardware Error Log and follow the procedures given in the appropriate DS1-BD/MM-DS1-BD Maintenance documentation for the listed error types.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals for a maximum of 5 times.
	FAIL	The far-end trunk did not respond to the seizure of the near-end trunk within the allowable time period. This test could have associated in-line errors in the error log. Enter the **list configuration board GGGVS** command. Eventually, the board and all of its ports will be taken out of service and extraneous on-board alarms will be generated. Replace the Media Module with a TN767C V3 or later. Verify that the 'Trunk Type' field on the 'Trunk Administration' screen matches the trunk type administered on far-end switch. Look for DS1-BD or MM-DS1 errors in the hardware error log. If present, refer to the DS1-BD (DS1 trunk Media Module) Maintenance documentation or to the MM-DS1 (MM-DS1 trunk Media Module) Maintenance documentation. Retry the test at 1-minute intervals for a maximum of 5 times.

2 of 3

Table 125: TEST #136 DS1 Tie Trunk Seizure Test *3 of 3*

Error Code	Test Result	Description/ Recommendation
2000	FAIL	Response to the seizure message was not received within the allowable time period. Enter the **list configuration board GGGVS** command. Eventually, the board and all of its ports will be taken out of service and extraneous on-board alarms will be generated. Replace the Media Module. Verify that the 'Trunk Type' field on the 'Trunk Administration' screen matches the trunk type administered on far-end switch. Look for MG-DS1 errors in the hardware error log. If present, refer to the MG-DS1 Maintenance documentation. Retry the test at 1-minute intervals for a maximum of 5 times.
	PASS	The trunk can be seized for an outgoing call.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Check to ensure that the board translations are correct. Use the **list config** command, and resolve any problems that are found. If the board was found to be correctly inserted in step 1, use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port. If this is not the case, check to see that there is a valid board inserted.
*Earlier G1 Software Versions reported Error Code 2053 as a FAIL.		

3 of 3

WAE-PORT (Wideband Access Endpoint Port)

Table 126: WAE-PORT (Wideband Access Endpoint Port)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run*	Full Name of MO
WAE-PORT	MINOR	test access-endpoint *extension* l	Wideband Access
WAE-PORT	WARNING	test access-endpoint *extension*	Endpoint Port
*For additional repair information, see also DS1-BD (DS1 Interface Media Module).			

Wideband Switching supports end-to-end connectivity between customer endpoints at data rates from 128 to 1536 kbps over T1 facilities and to 1984 kbps over E1 facilities. Communication Manager switching capabilities are extended to support wideband calls comprised of multiple DS0s that are switched end-to-end as a single entity.

Wideband Switching extends the Administered Connections feature to include non-signaling wideband access endpoints. Endpoint application equipment with direct T1 or E1 interfaces may connect directly to the switch's line-side facilities; application equipment without T1 or E1 interfaces requires a terminal adapter such as a DSU/CSU. The terminal adapter or endpoint application equipment is connected to the MM710.

These endpoints are administered as wideband access endpoints and have no signaling interface to switch; they simply transmit and receive data. (Some applications detect and respond to the presence or absence of data.) Calls are initiated from these endpoints using the Administered Connections feature.

Multiple access endpoints on one line-side MM-DS1 Media Module facility are separate and distinct within the facility. Endpoint application equipment must be administered to send and receive the correct data rate over the correct DS0s. All Administered Connections originating from wideband access endpoints use the entire bandwidth administered for the endpoint. An incoming call of a different data rate then that administered of the endpoint cannot be routed to the endpoint.

Although Wideband Access Endpoints are used primarily for line-side facilities, these endpoints can also be administered on network DS1 facilities to connect Communication Manager to non-switched network services, such as the Avaya fractional T-1 service. An example of this is the Avaya Static Integrated Network Access, where a trunk group to AT&T 4ESS Switched Services shares an access T-1 facility with a Wideband Access Endpoint. In this case, the Wideband Access Endpoint is connected to the AT&T fractional T-1 service, and it does not terminate on local endpoint equipment but is connected to a far-end CPE via the dedicated fractional T-1. All Wideband Access Endpoint functionality and operation is identical on both line-side and network facilities. However, because maintenance capabilities are limited to the Wideband Access Endpoint interface, and because faults can occur end-to-end, troubleshooting procedures based on an end-to-end view of the network is required.

Wideband access endpoint port maintenance provides a strategy to maintain a wideband access endpoint port via a port on the DS1 interface Media Module hardware. The maintenance strategy covers logging wideband access endpoint port hardware errors, running tests for port initialization, periodic and scheduled maintenance, demand tests, and alarm escalation and resolution. Two different port service states are specified in the wideband access endpoint port maintenance:

- *out-of-service*: the port is in a deactivated state and cannot be used for calls
- *in-service*: the port is in an activated state and can be used for calls

  If the DS1 Interface Media Module is out of service, all ports on it are taken out of service and a Warning alarm is raised.

Error Log Entries and Test to Clear Values

Table 127: Wideband Access Endpoint Maintenance Error Log Entries

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test access-endpoint *extension* sh r 1
18(a)	0	busyout access-endpoint	WARNING	OFF	release access-endpoint *extension*
130(b)		None	WARNING	ON	test access-endpoint *extension*
1793(e)		None			test board *GGGVSpp* long
3840(f)	Any	Port Audit and Update (Test #36)			

*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.

Notes:

- (a) The wideband access endpoint has been busied out by a **busyout access-endpoint** extension command. No calls can be made to this extension.
- (b) The Media Module has been removed or has been insane for more than 11-minutes. To clear the error, reinsert or replace the Media Module.
- (e) The Interface Media Module has failed. See MG-DS1.
- (f) The Port Audit and Update Test (#36) failed due to an internal system error. Enter **status access-endpoint** extension and verify the status of the port. If the wideband access endpoint port is out of service, enter **release access-endpoint** extension to put it back into service. Retry the test command.

Technician-Demand Tests: Descriptions and Error Codes

Always investigate tests in the order presented in the table below when inspecting errors in the system. By clearing error codes associated with the *NPE Crosstalk Test*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 128: Technician-Demand Tests

Order of Investigation	Short Test Sequence	Long Test Sequence	D/ND*
NPE Crosstalk Test (#6) **Note:** This Test ABORTS with code 1412 when run on a Avaya G350 Media Gateway system.		X	ND
Conference Circuit Test (#7) **Note:** This Test ABORTS with code 1412 when run on a Avaya G350 Media Gateway system.		X	ND
Port Audit and Update Test (#36)	X	X	ND
*D = Destructive; ND = Nondestructive			

Port Audit and Update Test (#36)

This test sends port level translation data from switch processor to the MG-DS1 Interface Media Module to ensure that the wideband access endpoint port's translation is correct.

Table 129: TEST #36 Audit and Update Test *1 of 2*

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
1006	ABORT	The port is out-of-service. If the port is busied out: Use **release access-endpoint <extension>** command to put the port back into in-service. Retry the test command. If the port is not busied out: Check the error and alarm logs for WAE-PORT and MM-DS1 errors and alarms and follow the recommended repair procedures.

1 of 2

Table 129: TEST #36 Audit and Update Test *2 of 2*

Error Code	Test Result	Description/ Recommendation
2000	ABORT	Response to the test request was not received within the allowable time period. Retry the command at 1-minute intervals a maximum of 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	Internal system error Retry the command at 1-minute intervals a maximum of 5 times.
	PASS	Port translation has been updated successfully.
Any	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. Ensure that the board translations are correct. Execute the **add ds1 GGGVS** command to administer the MG-DS1 interface if it is not already administered. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If this is the case, the board is shut down. Reseating the board will re-initialize the board. If the board was found to be correctly inserted in step 1, then use the **busyout board** command. Use the **reset board** command. Use the **release busy board** command. Use the **test board long** command. This should re-establish the linkage between the internal ID and the port.

2 of 2

XXX-BD (Common Port Media Module)

Table 130: XXX-BD (Common Port Media Module)

MO Name (in Alarm Log)	Alarm Level	Initial Command to Run *	Full Name of MO
XXX-BD**	MAJOR	test board GGGVS	Common Port Media Module Maintenance
XXX-BD**	MINOR	test board GGGVS	Common Port Media Module Maintenance
XXX-BD**	WARNING	test board GGGVS	Common Port Media Module Maintenance
Note: You must consult local records for the location and designation of the equipment rack where the G350 is mounted.			
**Refer to the appropriate Media Module documentation for the correct MO name displayed in this field. It usually ends with BD.			

Common Port Media Module Maintenance is a set of common tests used by all the Media Modules listed in the tables below. The XXX-BD designation is also used on SAT displays when **reset board** is entered with an empty Media Module slot, or with a Media Module type that is in conflict with the actual board type administered for that slot. All Media Module suffixes (B,C, D, and so forth) are supported by “XXX-BD.”

When any of the Common Port Media Modules are physically removed from the backplane, no alarm will be logged for approximately 11-minutes. (In the case of the MM712 Digital Line, MM720, and INTUITY AUDIX, approximately 21-minutes will elapse before an alarm is logged.) When a Media Module that has been removed is alarmed, the alarm type is minor and is classified as an on-board alarm. The time delay permits maintenance activity to be performed without triggering an additional alarm.

Alarms are logged against only those common port Media Modules on which ports have been administered. In a heavily loaded system, the interval between the removal of a Common Port Media Module and the logging of the alarm may be several minutes longer. Suffixes are not shown; for a list of all Media Modules supported, see the table in Chapter 2. Those that appear in **bold** type are documented separately under their own maintenance object name.

XXX-BD Common Media Modules

The following list of Media Modules are listed by apparatus code.

Table 131: XXX-BD Common Media Module

Apparatus Code	Name	Type
MM710	DS1/E1 Interface - T1, 24 Channel - E1, 32 Channel	Port
MM711	Analog Trunk and Line	Port
MM712	Digital Line, 8-Port, 2-Wire DCP	Port

Error Log Entries and Test to Clear Values

Table 132: Common Port Media Module Maintenance Error Log Entries *1 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
0*	0	Any	Any	Any	test board GGGVS sh r 1
1(a)	0	Media Gateway removed or SAKI Sanity Test (#53)	MINOR	ON	
18(b)	0	busy-out board GGGVS	WARNING	OFF	release board GGGVS
23(c)	0	None	WARNING	OFF	
125 (e)		None	MINOR	ON	
257	65535	Control Channel Test (#52)	MINOR	ON	test board GGGVS sh r 20
257 (g)	Any	None			
267	0	None	WARNING	ON	
513 (h)	Any	None	MINOR	ON	test board GGGVS sh
					1 of 2

Table 132: Common Port Media Module Maintenance Error Log Entries *2 of 2*

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
769 (i)	4358	None			
1281 (k)		Ringing Application Test (#51)	MINOR	ON	test board GGGVS r 2
1538 (l)	Any	None	WARNING/ MINOR	ON	
3840 (n)	Any	None			
3999 (o)	Any	None			
*Run the Short Test Sequence first. If all tests pass, run the Long Test Sequence. Refer to the appropriate test description and follow the recommended procedures.					
					2 of 2

Notes:

- (a) Error type 1 indicates the Media Module has stopped functioning or has been physically removed from the system. The alarm is logged approximately 11 minutes after removal of the Media Module or failure of the SAKI Sanity Test (#53).

  Check for the physical presence of the Media Module in the slot indicated by the alarm. If the Media Module is not present, insert one of the proper type. If the Media Module is present and its red LED is lit.

- (b) This error indicates the Media Module has been busied out. Release the Media Module via **release board GGGVS**.

- (c) The Media Module has been logically administered but not physically installed. The alarm should clear when the circuit pact is installed.

  If the Media Module is already installed:

  1. Run **test board GGGVS long** and look at any test failures or error codes generated.
  2. If the test does not clear error 23, then execute **reset board GGGVS** and run the long test again.
  3. If the reset/test does not clear error 23, replace the Media Module.

- (e) The Media Module physically installed in the slot does not match the type that is administered for that slot. Do one of the following:

  - Remove the incorrect Media Module and replace it with one of the type that is administered for that slot.
  - Use **change media module** to re-administer the slot so that it matches the board that is installed, and follow with **reset board**.

- (g) This error indicates transient communication problems with this Media Module. This error is not service-affecting and no action is required.
- (h) This error, when reported with Aux data in the range of 4352 to 4358, indicates that the Media Module has reported an on-board hardware failure. The Media Module will continuously test the hardware and report the results approximately every 10 minutes. If the hardware problem is resolved, the “leaky bucket” strategy should clear the alarm in approximately 30 minutes. However, if the alarm does NOT clear in 30 minutes, then the Media Module should be replaced.
- (i) This error can be ignored, but look for other errors on this Media Module.
- (k) This error indicates that no ringing current is detected. Run Test #51, Ringing Application Test, and follow the procedures for Test #51. This error is only applicable to Analog Line Media Modules.
- (l) The hyperactive Media Module is out-of-service and may exhibit one or more of the following symptoms:
  - The common Media Module level tests such as Test #51 are aborting with error code 2000.
  - The tests run on the ports of this Media Module are returning with a NO-BOARD.
  - A busy-out/release of the Media Module has no affect on test results.
  - A **list configuration** command shows that the Media Module and ports are properly installed.

  If this error happens again within 15 minutes, then replace the Media Module. If the XXX-BD is a Digital Line Media Module, then check the alarm level. If the alarm level is a WARNING, this indicates that users are probably causing the hyperactivity by playing with their digital stations. If the Media Module is really hyperactive then this alarm will be upgrade to a MINOR alarm within 1 hour. If the alarm level is a MINOR alarm, then replace the Media Module.
- (n) This error is not service-affecting and no action is required.
- (o) Error type 3999 indicates that the Media Module sent a large number of control channel messages to the switch within a short period of time. If error type 1538 is also present, then the Media Module was taken out-of-service due to hyperactivity. If error type 1538 is not present, then the Media Module has not been taken out-of-service, but it has generated 50% of the messages necessary to be considered hyperactive. This may be completely normal during heavy traffic periods. However, if this error type is logged when the Media Module is being lightly used, it may indicate a problem with the Media Module or the equipment attached to it.

Technician-Demand Tests: Descriptions and Error Codes

Always investigate tests in the order presented in the table below when inspecting errors in the system. By clearing error codes associated with the *NPE Audit*, for example, you may also clear errors generated from other tests in the testing sequence.

Table 133: Technician-Demand Tests

Order of Investigation	Short Test Sequence	Long Test Sequence	Reset Board Sequence	D/ND*
NPE Audit Test (#50) **Note**: This Test will ABORT with code 1412				
Ringing Application Test (#51) (a) **Note**: This Test will ABORT with code 1412				
Control Channel Looparound Test (#52)	X	X		ND
SAKI Sanity Test (#53) (b)		X	D	
Neon Test (#220) (c) **Note:** This Test will ABORT with code 1412	X	X		ND
*D = Destructive; ND = Nondestructive				

Notes:

- (a) This is only applicable to Analog Line Media Modules.
- (b) The SAKI Sanity Test is run on other Media Modules only when they are reset via the **reset board** command.
- (c) This is only applicable to MM711 Analog Line Media Modules.

Control Channel Looparound Test (#52)

This test queries the Media Module for its vintage to verify angel communication.

Table 134: TEST #52 Control Channel Looparound Test

Error Code	Test Result	Description/ Recommendation
None 2100	ABORT	System resources required for this test are not available. Retry the command at 1-minute intervals a maximum of 5 times.
	FAIL	The test failed because the Media Module failed to return the Media Module code or vintage. Retry the command for a maximum of 5 times. If the test still fails, use the **busyout board**, **reset board**, and **release busy board** commands, and then retest. If the problem continues, replace the Media Module. Run the test again.
	PASS	Communication with this Media Module is successful.
Any	NO BOARD	This is normal if the test is being done when (a) the board is not physically in the system or (b) the system is booting up. Otherwise, there is some inconsistency between the physical configuration and the data kept in the system. Verify that the board is physically in the system. Verify that the system is not in a stage of booting up. Retry the command at 1-minute intervals for a maximum of 5 times.

SAKI Sanity Test (#53)

CAUTION:
This test resets the Media Module

Table 135: TEST #53 SAKI Sanity Test

Error Code	Test Result	Description/ Recommendation
None	ABORT	System resources required for this test are not available. Retry the command at 1-minute intervals a maximum of 5 times.
1005	ABORT	If the Media Module needs to be reset, and if this is an Avaya G350 Media Gateway system, and the DS1 interface Media Module under test is providing timing for the platform, it cannot be reset without major platform disruptions (Note: For this type of system the sync timing source is local to the G350). Set the synchronization timing source to another DS1 interface Media Module located in the same G350 and retest. See Setting G350 synchronization on page 46. If the Media Module needs to be reset, then set synchronization to another DS1 interface Media Module or the Tone-Clock Media Module and try again. Refer to SYNC (Synchronization) Maintenance documentation.
1015	ABORT	Port is not out-of-service. Busy out the Media Module. Execute command again.
2100	ABORT	System resources required for this test are not available. Retry the command at 1-minute intervals a maximum of 5 times.
1	FAIL	The Media Module failed to reset.
2	FAIL	The Media Module failed to restart. Execute command again. If the problem persists, replace the Media Module.
	PASS	The Media Module initializes correctly. Run the short test sequence.
Any	NO BOARD	This is normal if the test is being done when (a) the board is not physically in the system or (b) the system is booting up. Otherwise, there is some inconsistency between the physical configuration and the data kept in the system. Verify that the board is physically in the system. Verify that the system is not in a stage of booting up. Retry the command at 1-minute intervals for a maximum of 5 times.

Chapter 4: License and authentication files

This chapter describes license and authentication files as they relate to the Avaya G350 Media Gateway controlled by an Avaya S8300, S8500, or S8700 Media Server.

For more detailed information on license and authentication files, refer to *Administrator's Guide for Avaya Communication Manager, 555-233-506*.

License and authentication file installation

Every S8300 Media Server and Local Survivable Processor requires a current and correct version of a license file and an Avaya authentication file in order to provide the expected call-processing service. The license file specifies the features and services that are available on the S8300 Media Server, such as the number of ports purchased. The license file contains a software version number, hardware serial number, expiration date, and feature mask. To add or remove call-processing features you must reinstall the license file. New license files may be required when upgrade software is installed.

The Avaya authentication file contains the logins and passwords to access the S8300 Media Server. This file is updated regularly by Avaya services personnel, if the customer has a maintenance contract. A valid authentication file must be present on the S8300 Media Server, or *all* access to Avaya Communication Manager from *any* login is blocked.

A new license file and the Avaya authentication file may be installed independently of each other or any other server upgrades.

In addition, to enable IPSec VPN, you must obtain and install a VPN license.

Downloading the license and authentication files

Use the License File Remote Feature Activation (RFA) to obtain the license and Avaya authentication files, including a VPN license when applicable. RFA is a Web-based application, available to Avaya employees and authorized Business Partners, that enables the creation and deployment of license files for all media server configurations. The license file enables the software category, release, features, and capacities. License files are created using SAP order information and/or current customer configuration information.

Without a valid license installed or a mismatched license:

- The system generates a major alarm.
- Depending upon the nature of the error, a 10-day countdown timer starts (this was formerly a 6-day period), but call processing continues uninterrupted.
- If the countdown timer expires, the switch enters No License Mode and generates another major alarm.

Note:

The *init* login can no longer change the customer options, offer option, or special applications forms.

Once the Avaya authentication files are installed, Avaya services logins to the S8700 Media Server are protected by a challenge/response system called Access Security Gateway (ASG). The ASG challenge/response protocol confirms the validity of each user, reducing the opportunity for unauthorized access.

Before starting the installation or, ideally, before coming on site, the license and Avaya authentication files may be downloaded to the services laptop. The license and Avaya authentication files are routinely installed during the installation process.

To access the RFA application, you must take the RFA online training and pass the online test.

RFA information requirements for new installations

You need the following information before going to the RFA web site:

- Your personal Single Sign-On (SSO) for RFA web site authentication login
- SAP order number
- Required customer information
- Serial number of the G350 Media Gateway
- Access to the RFA Information page for these items (if not already installed on your PC):
  - Internet Explorer 5.0 or higher installed on the services laptop
  - Intranet access to the RFA Web site.

Go to the RFA web site

The RFA web site automates some of the installation procedures, including generating license and Avaya authentication files.

To download the customer’s license and authentication files to your laptop:

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and authentication files (for example, C:\licenses).
2. Access the Internet from your laptop and go to http://rfa.avaya.com.

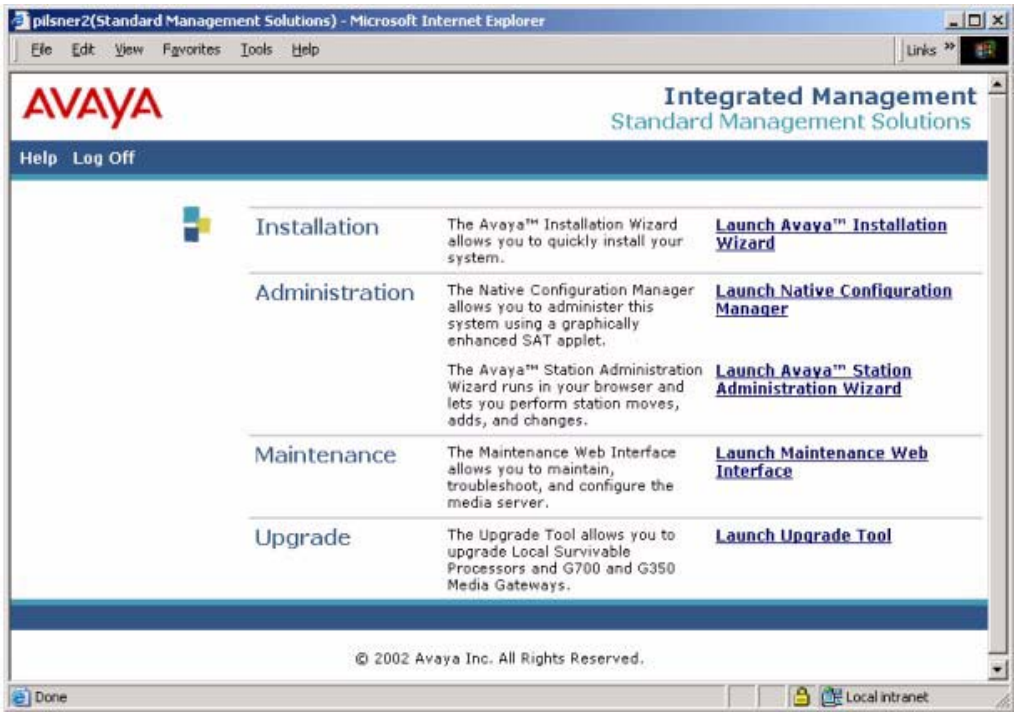
3. Use the System ID or the SAP ID of the customer to locate the license and authentication files for the customer.
4. Check that the license and authentication files are complete.
5. If the files are not complete, complete them. You might need to add the serial number of the customer's G350.
6. Use the download or e-mail capabilities of the RFA web site to download the license and authentication files to your laptop.

Installing license and authentication files

To install the license and authentication files:

1. Access the Maintenance web pages part of Avaya Integrated Management (AIM) from your laptop, using IP address 192.11.13.5.
2. Logon at the Avaya Integrated Management Logon screen. The main menu for Avaya Integrated Management appears.

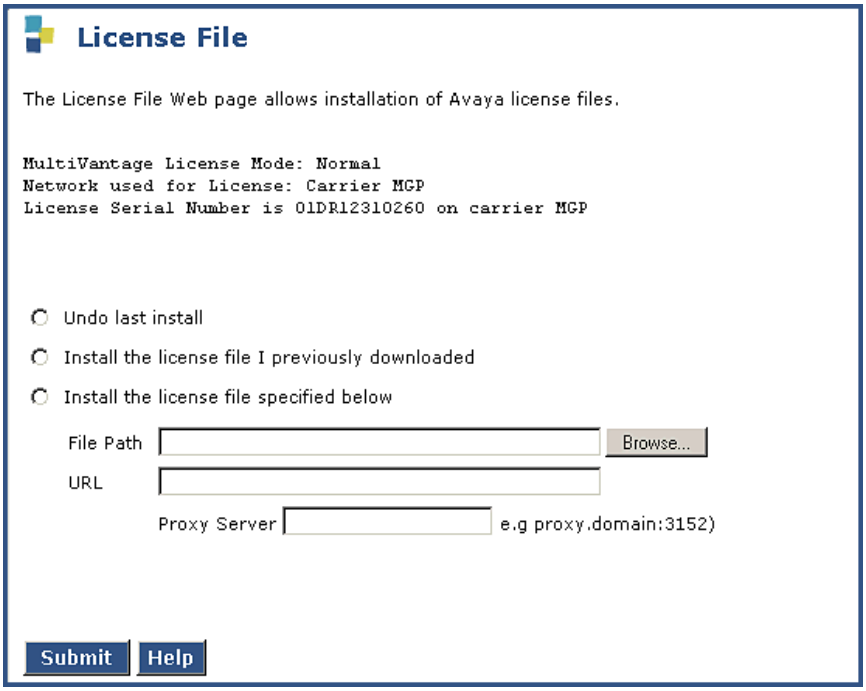
Figure 12: Integrated Management Main Menu



3. From the Integrated Management main menu, select Launch Maintenance Web Interface. The Maintenance Web Pages Notice page appears, with a navigation menu at the left.

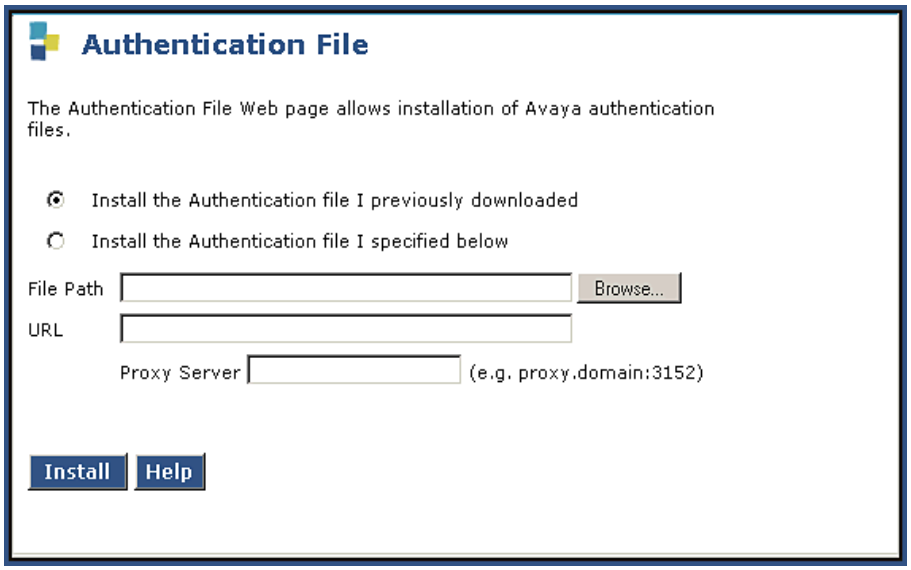
4. From the navigation menu of the Maintenance Web Pages, select **Security** > **License File**. The License File web page appears.

Figure 13: License File Web Page



5. Select **Install the license file specified below**.
6. Browse to the customer's license file (.lic), which you downloaded from the RFA web site.
7. Click **Submit**. A message appears telling you your installation was successful.
8. From the navigation menu, select **Security > Authentication File**. The Authentication File web page appears.

Figure 14: Authentication File Web Page



9. Select **Install the Authentication file I specified below**.
10. Browse to the customer's authentication file (.pwd), which you downloaded from the RFA web site.
11. Click **Install**. A message appears telling you your installation was successful.

    Installing the Avaya authentication file removes all default passwords and establishes new ones. After the installation, services logins specific to the media server are protected through Access Security Gateway (ASG), which means a craft login will be challenged.

License files for different configurations

License files are assigned differently depending on the Media Server and Avaya G350 Media Gateway configuration.

S8300 Media Server

When the system configuration is a G350 with an S8300, the S8300 is a Linux-based processor running Communication Manager. The serial number of the G350 in which the S8300 is inserted is used in the license file for identification.

External Media Server (S8500, S8700)

When the Communication Manager is running on an External Media Server, such as an S8700, that platform's hardware is used for license file authentication. In this configuration, a G350 does not require a separate license file and is thought of as an extension of the server's platform. Licensing is handled by the S8500 or S8700 Media Server.

Survivable configuration

In a survivable configuration, the S8300 Media Server is configured as a Local Survivable Processor — referred to as an LSP. The LSP is present on the G350, but Communication Manager is not active, and runs in a special survivable mode. The LSP provides service to a subset of endpoints in the event that the G350 cannot be served by its primary Media Server.

Each S8300 configured as an LSP has its own license file that contains the serial number of the G350 into which the LSP is physically inserted. As soon as the LSP becomes active and begins providing service as the Media Server, it invokes License-Error mode. The LSP can remain in License-Error mode for a maximum of ten days. If the LSP is still acting as the active server after that time, it enters No-License mode.

A new display-only field has been added to the *OPTIONAL FEATURES* section of the **system-parameters customer-options** form. This field is used to indicate that the switch is an S8300 functioning in Local Survivable Processor mode. This field is modified only via the license file and is "display only" on the **system-parameters customer-options** form. A new display-only field name is included called *Local Spare Processor*.

License file modes

License files for the Avaya S8300 Media Server in an Avaya G350 Media Gateway function in the following three modes:

- License-Normal Mode
- License-Error Mode
- No-License Mode

License-Normal mode

This is the desired mode of operation for a stable device. In this mode, a license is properly installed, the license contains a serial number that matches the G350's, the license is not expired, and the feature usage does not exceed limits set in the license.

License-Error mode

This is a warning mode. In this mode, call processing is supported, a major alarm is declared, and a ten-day timer begins. If this timer expires, No-License Mode is invoked.

Clear License-Error Mode by correcting the error that caused entry into License-Error Mode, or by installing a valid license that is consistent with the configuration of the switch.

This is caused when:

- A survivable processor begins to provide service, which causes a major alarm
- The serial number in the license file does not match the serial number of the G350 into which the S8300 is physically inserted

To resolve this problem:

- Check the networking
- Check the serial numbers

Access the following sections of the Web Interface:

- Security – View License Status
- Server Configurations and Upgrades – View Serial Number

No-License mode

In this mode, call processing continues, but the system operates in No-License Mode.

Clear No-License Mode by correcting the error that caused entry into No-License Mode, or by installing a valid license that is consistent with the configuration of the switch.

To resolve this problem:

- Check the networking
- Check the serial numbers

Access the following sections of the Web Interface:

- Security – View License Status
- Server Configurations and Upgrades – View Serial Number

License and Options Forms interactions

The software license contains a set of information known as a feature mask. The content of the feature mask controls what features are enabled or may be enabled on the product. There are several types of entries in the feature mask:

- Type I Entry
- Type II Entry
- Type III Entry

Type I entries

Type I entries relate to those types of features that have a simple on/off state. An example is “DCS Call Coverage.” It is either enabled or not. Each Type I entry has two variables associated with it:

- A value
- A lock

Variables are always locked either On of Off by the License File. Four combinations are possible with meanings as shown in Table 136: Type I Feature License Behavior on page 271.

Table 136: Type I Feature License Behavior

License Content		Consequence	
Value	**Lock**	**Feature Status**	**Options* Screen**
On	Unlocked	Set by translation via login. If no translation, feature is enabled.	init and dadmin may administer this feature.
On	Locked	Translation is always ignored. Feature is enabled any time translations are loaded.	init and dadmin may turn this feature off and then back on, but when the switch is rebooted or translation loaded, the feature will be on. i.e., login affects current value in memory only.
Off	Unlocked	Set by translation via login. If no translation, feature is disabled.	init and dadmin may administer this feature.
Off	Locked	Translation is always ignored. Feature is disabled any time translations are loaded.	The entry for this feature is display only on the options form. It may not be turned on via any login.

*offer-options, customer-options, and special applications forms

Type II entries

Type II entries relate to those types of features that have a numeric value. An example is “Logged-in ACD Agents.” Each type II entry has two values associated with it, a lower limit value (V1), and an upper limit value (V2). V1 is never greater than V2. The following conditions are possible as shown in Table 137: Type II and Type III Feature License Behavior on page 272.

Table 137: Type II and Type III Feature License Behavior

License Content	Consequence	
V1 and V2	**Feature Status**	**Options* Screens**
V1 less than V2	If no translations are present or if translation value is less than V1 or greater than V2, feature has value V1. If translations are present and have a value from V1 to V2, then feature has value from translation.	init and dadmin can administer this feature to any value from V1 to V2.
V1equal to V2	Feature has value V1.	The entry for this feature is displayed only on the options form. It may not be set via any login.
V1 greater than V2	This is not a valid state. The license tools should prohibit this condition. License is invalid.	License is invalid. If this condition reaches the switch, the effective value is zero.
*offer-options, customer-options, and special applications forms		

Type III entries

Type III entries relate to those types of features that have a product ID, a release number, and a numeric value. An example is “IP_Agent.” Just as for Type II features, the numeric value for each type III entry has two values associated with it, a lower limit value (V1), and an upper limit value (V2). V1 is never greater than V2. See Table 137: Type II and Type III Feature License Behavior on page 272.

Chapter 5: Access and login procedures

This chapter describes the various ways of connecting to, and logging into, the S8300 Media Server and the Avaya G350 Media Gateway. Use this chapter as a reference for the other chapters in this book.

The procedures in this chapter assume that you are connecting to the S8300 and/or the G350 with an Avaya Services laptop. However, the methods apply for any type of PC.

This chapter contains the following sections:

Connection overview

There are several methods of connecting to the Avaya G350 Media Gateway and the S8300 Media Server, as shown in Figure 15: Summary of S8300 and G350 Access Methods and Tasks on page 275. Choose the method and tools appropriate for your maintenance task.

Initial configuration and maintenance of the S8300 Media Server

Connect to the S8300 Media Server using a laptop connected to the Media Server's Services port.

Onsite tasks

1. Configure Media Server
2. Install license and authentication files, and upgrade software
3. Verification testing
4. Run diagnostics
5. Upgrade software and configuration

Tools

- Media Server Web Interface
- Command Line Interface
- System Access Terminal (SAT)

System Admin computer or technician laptop administration via corporate LAN

Connect to the Avaya G350 Media Gateway using a computer over the corporate LAN. The LAN is connected to the Avaya G350 Media Gateway's Ethernet port.

Tasks

1. Backup and restore data
2. Perform upgrade and configuration
3. Administer network
4. Administer telephony features

Tools

- Media Server Web Interface
- Avaya Site Administration
- Avaya Device Manager
- System Access Terminal (SAT)

Remote access to S8300

Connect to the S8300 remotely using a USB modem plugged in to the Media Server's USB port.

Tasks

1. Diagnosis of Media Server
2. Alarm notification

Remote access to the G350 Media Gateway

Connect to the G350 remotely using a USB modem plugged in to the USB port of the G350.

Tasks

1. Diagnosis of media gateway
2. Remote administration of media gateway

Initial configuration and maintenance of Media Gateway (no S8300)

Connect to the Avaya G350 Media Gateway directly using a laptop connected to the Console port.

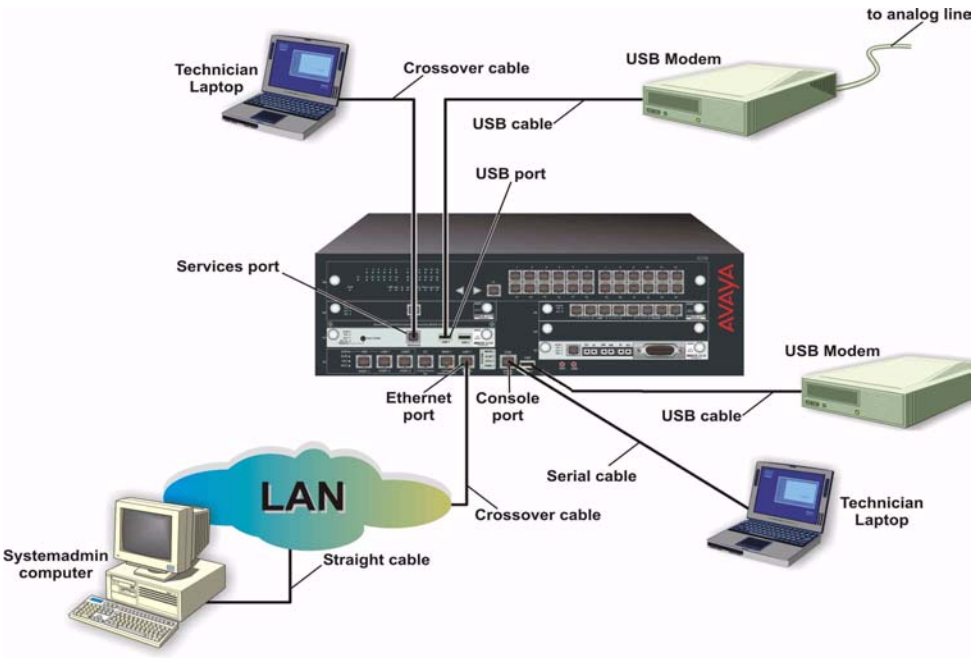
Onsite Tasks

1. Configure master
2. Configure Media Gateway, Media Modules, and ports
3. Update configuration
4. Run diagnostics

Tools

- Command Line Interface

Figure 15: Summary of S8300 and G350 Access Methods and Tasks



Connecting the G350 to the customer LAN

If you are providing maintenance for a G350 that does not have an internal S8300, you may need to connect the G350 to the customer's LAN. There are various ways that the G350 is connected to the customer's LAN, depending the G350's configuration.

- If you have a G350 by itself, or a G350 with a router, the G350 connects to the LAN via the ETH LAN port.
- If you have a G350 with a switch, the MM314 Media Module, installed in the G350, connects to the LAN via the ETH LAN port or one of the MM314 Ethernet ports.
- If you have a stand-alone configuration, the G350 is the LAN switch and the WAN router. For example, slot V6 of the G350 is loaded with a MM314 Media Module with 24 Power-over-Ethernet ports.

Connecting a laptop to the S8300 Services port

Connecting a laptop directly to the S8300 Services port requires you to configure the laptop with a special network configuration.

Note:

Avaya Service technicians can use the NetSwitcher program to configure alternate network profiles so they can easily connect to a number of different systems. NetSwitcher configures a profile for each type of system for easy future access without requiring you to reset TCP/IP properties or browser settings manually. NetSwitcher is available from an Avaya Services CTSA.

Configuring the laptop network settings

A laptop connected directly to the Services Ethernet interface on the S8300 Media Server requires a specific configuration as described in this section.

The network settings must be configured as follows:

- *TCP/IP properties* – set the laptop's TCP/IP properties as follows:
  - IP address: **192.11.13.5**
  - Subnet mask: **255.255.255.252**
- *Browser settings* – configure the browser for a direct connection to the Internet. Do *not* use proxies.
- *Server address* – access the S8300 media server using the URL http://192.11.13.6.

The names of the dialog boxes and buttons vary on different operating systems and browser releases. Use your computer's help system if needed to locate the correct place to enter this information.

The S8300 Media Server uses the same access configuration as an Avaya S8100 Media Server with a CMC1 or G600 Media Gateway. If you already have a NetSwitcher profile for the S8100 Media Server (formerly called DEFINITY One), try using that profile first before configuring a new one.

Setting TCP/IP properties in Windows

TCP/IP administration varies among Windows systems as described below.

Note:

Make a record of any IP addresses, DNS servers, or WINS entries that you change when you configure your services computer. Unless you use the NetSwitcher program or an equivalent, you will need to restore these entries to connect to other networks.

To check Your Version of Windows:

1. Log in to your laptop, and double-click the **My Computer** icon on your desktop.

   The My Computer window opens.

2. Click **Help** on the My Computer window's toolbar.

   The Help menu opens and displays the version of Windows installed on your laptop.

3. Follow one of the two procedures below, depending on your operating system.

To change TCP/IP Properties and Network Settings (Windows 2000 and XP):

1. Right-click My Network Places on your desktop or under the Start menu in XP.
2. Select **Properties** to display the Network and Dial-up Connections window.

   Windows should have automatically detected the Ethernet card in your system and created a LAN connection for you. More than one connection may appear.

3. Right-click the correct **Local Area Connection** from the list in the window.
4. Select **Properties** to display the Local Area Connection Properties dialog box.
5. Select **Internet Protocol (TCP/IP)**.
6. Click the **Properties** button. The Internet Protocol (TCP/IP) Properties screen appears.
7. On the General tab, select the radio button **Use the following IP address**. Enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

Note:

Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.

8. **Disable DNS service as follows:**
   a. Click the radio button labeled **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
   b. Click the **Advanced** button at the bottom of the screen. The Advanced TCP/IP Settings screen appears.
   c. Click the **DNS** tab. Verify that no DNS server is administered (the address field should be blank).
9. Disable WINS Resolution as follows:
   a. Click the **WINS** tab. Make sure WINS is not administered (the address field should be blank).
   b. Click **OK**. If warned about an empty primary WINS address, click **Yes** to continue.
10. Click **OK** twice to accept the address information and close the TCP/IP and Local Area Connection Properties dialog boxes.
11. Reboot the system if directed to do so.

    After you have made these changes to your computer's network configuration information, the Network and Dial-up Connections window shows the status of the Local Area Connection:

    - Enabled appears when the laptop's Ethernet cable is connected to the server.
    - Disabled or unplugged appears if the NIC is not connected to anything.

To change TCP/IP properties (Windows 95, 98, NT 4.0, and Millennium Edition [ME]):

1. Access your computer's network information. On your desktop:
   - *Windows 95, 98, and NT:* Right-click **Network Neighborhood**.
   - *Windows Me:* Right-click **My Network Places**.
2. Select **Properties** to display the Network dialog box.
3. Locate the TCP/IP properties as follows:
   - *Windows 95, 98, and Me:* On the **Configuration** tab, scroll through the installed network components list to the TCP/IP part of the devices list. Select the TCP/IP device that corresponds to your Ethernet card.
   - *Windows NT:* On the Protocols tab, select **TCP/IP** in the installed network components list.
4. Select the **Properties** button.

5. In the TCP/IP Properties box, click the **IP Address** tab.
6. Click the radio button to **Specify an IP address**, and enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

   Note:

   Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.
7. Disable DNS service as follows:
   - *Windows 95, 98, and Me:* Click the **DNS Configuration** tab. Verify that the **Disable DNS** radio button is selected.
   - *Windows NT:* Click the **DNS** tab.
     - If any IP addresses appear under DNS Service Search Order, make a note of them in case you need to restore them later.
     - Select each IP address in turn and click the **Remove** button.
8. Disable WINS Resolution as follows:
   - *Windows 95, 98, and Me:* Click the **WINS Configuration** tab. Verify that the **Disable WINS Resolution** radio button is selected.
   - *Windows NT:* Click the **WINS Address** tab.
     - If any IP addresses appear for the Primary and Secondary WINS servers, make a note of them in case you need to restore them later.
     - Clear each server entry.
     - Clear the check box for **Enable DNS for WINS Resolution**.
9. Click OK twice to accept the address information and close the Network dialog box.
10. Reboot the system if directed to do so.

To disable/bypass proxy servers in browser:

If you are connecting a laptop directly to the Services Ethernet interface on the S8300 faceplate, you must either disable or bypass proxy servers as described below.

Note:

The Microsoft Internet Explorer (IE) browser is recommended. If you use IE, it must be version 5.5 or higher. You can use Netscape, but some features of the web interface may not work properly. If you use Netscape, it must be version 6.2 or higher.

To check or change proxy settings:

1. Open your Internet browser.
2. Verify that you have a direct connection with no proxies as follows:

For Internet Explorer

1. Select **Tools > Internet Options**.
2. Click the **Connections** tab.
3. Click the **LAN Settings** button.
4. If **Use a proxy server for your LAN** is not selected, no change is necessary; click **Cancel** to exit.
5. If **Use a proxy server for your LAN** is selected, you can:
   - Deselect it and click **0K** to exit;
   - Or, you can leave it selected and configure your browser to bypass the proxy server whenever you are connected to the S8300 services port as follows:
     - Click **Advanced.**
     - Type **192.11.13.6** in the Exceptions box. If there are other entries in this box, add to the list of entries and separate entries with a ";".
     - Click **OK** to exit.

For Netscape

1. Select **Edit > Preferences**.
2. Under Category, click **Advanced**.
3. Click **Proxies**.
4. If **Direct connection to the Internet** is selected, no change is necessary; click **Cancel** to exit.
5. If **Direct connection to the Internet** is not selected, you can:
   - Select it and click **OK** to exit;
   - Or, you can leave it unselected and configure your browser to bypass the proxy server whenever you are connected to the S8300 services port as follows:
     - Select **Manual Proxy Configuration** and click **View.**
     - Type **192.11.13.6** in the Exceptions box (or in the **No Proxy for:** box in later versions of Netscape). If there are other entries in this box, add to the list of entries and separate entries with a ";".
     - Click **OK** to exit.

Connection methods

Connect laptop to Services port of S8300

To connect your laptop directly to the S8300 Media Server:

1. Make sure your laptop meets the hardware and software requirements.
2. Plug an Ethernet crossover cable (MDI to MDI-X) into the 10/100 BaseT Ethernet network interface card (NIC) on your laptop.
   - Crossover cables of various lengths are commercially available.
   - See Table 138: Crossover cable pinout chart on page 281 for pinout connections if needed. Crossover of the transmit and receive pairs (as shown) is required.

Table 138: Crossover cable pinout chart

Pin to Avaya S8300 Media Server's Services Ethernet interface	connects to	Pin to laptop's Ethernet card
8		8
7		7
6		2
5		5
4		4
3		1
2		6
1		3

3. Connect the other end of the crossover cable to the Services port on the front of the S8300.
4. If your laptop is configured with the correct network settings, you can now open your Internet browser or start a Telnet session and log in. When accessing the server from a directly connected laptop, always type the following IP address in the browser's Address or Location field to access the server: **192.11.13.6.**

Connect laptop to the G350 Serial port

To configure a G350 that *does not have an S8300*, you may need to set up a direct connection from your laptop's serial port to the G350 Console (serial) port.

To connect a laptop directly to the serial port on the Avaya G350 Media Gateway:

1. Connect the RS-232 serial cable and DB-9 adapter cable provided with the G350 between your laptop and the G350:
   - Attach one end of the RS-232 cable to the RJ-45 jack on the front of the G350. The serial port is at the bottom of the front of the chassis in the center, labeled **CONSOLE**.
   - Plug the other end of the RS-232 cable into the RJ-45 jack on the DB-9 adapter cable.
   - Connect the other end of the DB-9 adapter cable to the 9-pin serial port on your laptop.
2. Use a serial-connection program such as HyperTerminal to access the G350. Set the serial port speed to:
   - 9600 baud
   - 8 data bits
   - no parity
   - 1 stop bit

Connect laptop to customer LAN

To connect to the customer's LAN, either on site or remotely over the Internet, your PC must be assigned an IP address on the LAN. The IP address can be a static address on the customer's LAN that you enter in the TCP/IP properties or it can be assigned dynamically with DHCP. Ask the customer how they want you to make the connection.

Connect the external modem to the S8300 Media Server

Each S8300 Media Server requires a Universal Serial Bus (USB) modem for maintenance access and to call out an alarm. The external modem may be connected to the S8300 Media Server through a universal serial bus (USB) connection, providing dial-up access. Additional requirements include:

- The modem requires its own external analog line.
- The modem type is not optional and must be the specific modem that is shipped with the S8300.

- The remote connection should support a data speed of at least 33.6 Kbps.
- The remote PC must be administered for PPP connections in order to connect through a modem.

A dial-up connection is typically used only for services support of the server, not for routine administration. If the Server is administered to report OSS alarms, it uses the same line for alarm notification. The server cannot report any new alarms while this line is in use.

To connect the external modem to the S8300 Media Server:

1. Connect one end of the modem's USB cable to an available USB port on the S8300 Media Server's faceplate. Either USB1 or USB2 can be used.
2. Connect the other end of the cable to the external modem.
3. Connect the modem to an external analog line.

   Note:

   The modem that is shipped with the S8300 obtains its power from the USB interface. There is no power connection.
4. Verify operation as instructed by the modem's documentation.
5. To enable the modem, access the S8300 Media Server's Maintenance Web Pages (see Log in to the S8300 Web Interface from your laptop on page 289), and click Modem under the Security heading on the main menu.

   The system displays the Modem window.
6. Click the radio button for one of the following:
   - Enable modem for one incoming call — use this option if you want to provide one-time access to the Media Server over the modem.
   - Enable modem for unlimited incoming calls — use this option if you want to provide regular dial-up access to the Media Server for Services personnel or some other reason.

   The modem is now ready to receive calls.

Use Windows for modem connection to the Media Server (Windows 2000 or XP)

To use Windows for a modem connection:

Note:

The remote dial-up PC must be configured for PPP access. Also, Avaya Terminal Emulator does *not* support Windows XP.

1. Right-click **My Network Places** and click **Properties**.
2. Click **Make New Connection** and follow the Network Connection Wizard.

3. Select **Dial-up to private network** on the **Network Connection Type** screen.

   Note:

   If your system has more than one modem, you may be requested to select the device. If so, select the modem you are using to dial out.

4. In the **Phone number** field, enter the appropriate telephone number inserting special digits such as 9 and 1 or *70, if necessary.
5. On the Connection Availability screen, click **For all users** or **Only for myself**, as appropriate.
6. On the Completing the Network Connection Wizard screen, type the name you want to use for this connection. This name will appear in the Network and Dial-up Connections list.
7. Check the **Add a shortcut to my desktop**, if desired, and click **Finish**.
8. If a Connect screen appears, click **Cancel**.

Configure the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA)

To configure the remote PC for PPP modem connection:

1. On your PC's desktop, right-click **My Network Places** and click **Properties**.

   The system displays the Network and Dial-up Connections window.

2. Double-click the connection name you made in the previous task, Set up Windows for Modem Connection to the Media Server (Windows 2000 or XP).

   Note:

   Depending on your system, the Connect window may appear. If so, click **Properties**.

3. Click the **Security** tab.
4. Select the **Advanced (custom settings)** radio button.
5. Check the **Show terminal window** check box.
6. Click the **Networking** tab.
7. In the Components box, verify that Internet Protocol (TCP/IP) and Client for Microsoft Networks are both checked.
8. Select Internet Protocol (TCP/IP) and click **Properties**.
9. Click the **Advanced** button.
10. Clear the **Use default gateway on remote network** box.
11. Click **OK** three times to exit and save the changes.

Use Windows for PPP modem connection (Windows 2000 or XP)

Note:

Access to the system via PPP modem connection may require RAS access and ASG Mobile access.

To use Windows for PPP modem connection (Windows 2000 or XP):

1. Return to the Network and Dial-up Connections window and right-click the connection you just created.
2. Select **Connect**.
3. Leave the User Name, Password, and Domain fields blank. If the Dial field is blank, enter the appropriate telephone number.
4. Click the Dial button. When the media server's modem answers, the system displays the After Dial Terminal window.
5. Log on to the LAN.
   a. Enter your remote access login name and password.
   b. When the **Start PPP Now!** message appears, click **Done**.

      The system displays a small double-computer icon in the lower right portion of your screen.
6. Double-click the double-computer icon.

   The system displays the connection's Dialup Status box.
7. Click on the Details tab.
8. Note the Server IP address.
9. Open a telnet session to the S8300:

   Type **`telnet <ip-address>`**, where <*ip-address*> is the IP address of the S8300 as noted in the Dialup Status box from Step 8.
10. Access SAT or use the CLI commands as needed.

Use Avaya Terminal Emulator for LAN connection to Communication Manager

You can download the Avaya Terminal Emulator from the main menu for the VisAbility™ Management Suite. Simply click **Download** next to the Administration menu item and follow the instructions.

Once the Terminal Emulator is installed on your PC, use the following steps to establish a LAN connection to your Media Server.

To establish a LAN connection to the Media Server:

1. Double-click the Terminal Emulator icon on your desktop. Alternatively, go to the Start menu, select Programs, then select Avaya, and finally select Terminal Emulator.

   The system displays the Terminal Emulator.

2. From the menu bar across the top of the screen, select **Phones**, then select **Connection List**.

   The system displays the Connections window.

3. From the menu bar across the top, select **Connection**, then select **New Connection**.

   The system displays the Connection Settings window.

4. Put in a name for the connection. Usually, this will be the name of your Media Server.

5. In the Host window, click **Telnet**.

6. Click the **Emulation** tab at the top.

   The system displays the Emulation tab.

7. From the Emulator drag down box, select the emulator you desire, usually 513BCT (default), AT&T 4410, AT&T or DECVT100.

8. In the Keyboard window, select **pbx**.

9. Click the **Network** tab.

   The system displays the Network tab.

10. In the IP address field, type the IP address of the Media Server.

11. In the TCP/IP port number field, leave **23** if you want to log in at the Linux command line. Type **5023** if you want to log in directly to the Communication Manager SAT command line.

12. Click **OK**.

    The Connection Settings window disappears.

13. On the Connections window, double-click the name of the connection you just set up.

    If you used port 5023, the login prompt for Communication Manager appears. If you used port 23, the login prompt for the S8300 Linux software appears.

14. Log in to Communication Manager to access the SAT command prompt screen. If you are logging in as *craft*, you log in to the S8300 Linux software. Then see Open the Communication Manager SAT screens on page 290.

Use Avaya Terminal Emulator for modem connection to Communication Manager

Once the Terminal Emulator is installed on your PC, and you have a modem attached and configured to both your PC and the Media Server, use the following steps to establish a modem connection to your Media Server.

To establish a modem connection to the Media Server:

1. Double-click the Terminal Emulator icon on your desktop. Alternatively, go to the Start menu, select Programs, then select Avaya, and finally select Terminal Emulator.

   The system displays the Terminal Emulator.

2. From the menu bar across the top of the screen, select **Phones**, then select **Connection List**.

   The system displays the Connections window.

3. From the menu bar across the top, select **Connection**, then select **New Connection**.

   The system displays the Connection Settings window.

4. Put in a name for the connection. Usually, this will be the name of your Media Server.
5. In the Host window, click **Telnet**.
6. Click the **Emulation** tab at the top.

   The system displays the Emulation tab.

7. From the Emulator drag down box, select the emulator you desire, usually 513BCT (default), AT&T 4410, AT&T or DECVT100.
8. In the Keyboard window, select **pbx**.
9. Click the **Modem** tab.

   The system displays the Modem tab.

10. In the IP address field, type the IP address of the connection's Dialup Status box as noted in Step 8 of the above procedure.
11. In the TCP/IP port number field, leave **23** if you want to log in at the Linux command line. Type **5023** if you want to log in directly to the Communication Manager SAT command line.
12. In the **Modem** field, use the drag down box to select the type of modem that your PC uses.
13. In the **Serial port** field, select the COM port you are using for your modem connection.
14. In the **Baud rate** field, select **9600** from the drag down box.
15. Click the Dial Numbers tab.

    The system displays the Display Numbers tab.

16. Type the phone number of the Media Server, as appropriate. Enter 1 in the **Country Code** field for long-distance.

17. Click **OK**.
18. On the Connections window, double-click the name of the connection you just set up.

    The PC dials up the Media Server, and when connected, the login prompt for Communication Manager software appears.
19. Log in to Communication Manager to access the SAT command prompt screen.

    If you are logging in as *craft*, you log in to the S8300 Linux software. Refer to Open the Communication Manager SAT screens on page 290.

Log in methods

This section describes how to log on to the Avaya G350 Media Gateway or the S8300 Media Server using Telnet or the built-in Web Interface and how to start a SAT session. These procedures assume:

- You have a crossover cable directly connected from your laptop to the Services port on the Media Server and your laptop is configured for a direct connection
- Or, you are connected to the S8300 Media Server over the customer's LAN, either remotely or on site. In this case, your laptop must be configured to connect to the customer's LAN and you would use the LAN IP address of the S8300 instead of 192.11.13.6.

The last procedure in this section describes logging in to the Layer 2 interface on the media gateway when you have a direct serial connection to the G350 Console port.

Log in to the Media Server from your laptop using Telnet

To run Telnet:

1. Make sure you have an active Ethernet or serial connection from your computer to the Media Server.
2. Access the Telnet program; for example:
   - On a Windows system, go to the **Start** menu and select **Run**.
   - Type **telnet 192.11.13.6** to access the media server CLI.
3. When the **login** prompt appears, type the appropriate user name (such as **cust** or **craft**).
4. When prompted, enter the appropriate password.
5. If you log in as **craft**, you are prompted to suppress alarm origination. Generally you should accept the default value (yes).

6. Enter your terminal type. Accept the default value, or enter the appropriate type for your computer. For example, you may use type **ntt**, a terminal type available for Windows NT4.0 or Windows 98. For Windows 2000, use **w2ktt**.
7. If prompted for a high-priority session, typically answer **n**.

   The system displays the Telnet prompt. It may take the form <*username@devicename*>.

Log in to the S8300 Web Interface from your laptop

To run the Web Interface:

1. Open Internet Explorer (5.5 or later) on your computer.
2. In the Address (or Location) field of your browser, type the **192.11.13.6** (or, for a LAN connection, the IP address of the media server on the customer LAN) and press **Enter**.

   If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate.

   The system displays the Welcome screen.
3. Click the **Continue** button.
4. Accept the server security certificate to access the Login screen.

   The system displays the Login screen.
5. Log in as **craft**.

   The system displays the main menu for the VisAbility™ Management Suite.
6. Click on the link for **Launch Maintenance Web Interface**.

   The system displays the S8300 main menu in the left panel and a usage-agreement notice in the right window.
7. Check the top of the right panel.
   - The Avaya Media Server you are logged into is identified by name and server number.
   - The S8300 Media Server number is always 1.

Open the Communication Manager SAT screens

To run Communication Manager SAT:

1. If you already have a valid Telnet session in progress, access the SAT program by typing **`sat`** or **`dsat`** at the Telnet prompt.
2. Log in to the S8300 as **craft**.

   Enter your login confirmation information as prompted:

   - *Password prompt.* Type your password in the Password field, and click Login or press **Enter** again.
   - *ASG challenge*. If the login is Access Security Gateway (ASG) protected, you will see a challenge screen. Enter the correct response and click Login or press **Enter**.
3. Enter your terminal type. Accept the default value, or enter the appropriate type for your computer. For example, you may use type **ntt**, a terminal type available for Windows NT4.0 or Windows 98. For Windows 2000, use **w2ktt**.

   The system displays the SAT interface.
4. Enter SAT commands as appropriate.

Note:

You can also access the SAT program using the dadmin login. For instructions, see Chapter 1 of *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server*, 555-234-100.

Log in to the G350 Media Gateway interface with a direct connection to the Services port

Use this procedure to log in to the G350 Media Gateway interface when you have a direct connection with your laptop to the S8300 Services port.

Note:

If you are upgrading an S8300/G350 remotely, connect to the customer LAN and telnet to the IP address of the G350 interface. The IP address is the address assigned on the customer LAN, not 192.11.13.6.

To log in to the G350 interface via the Services port:

1. With a direct connection to the S8300 services port, telnet to the S8300 IP address:

   Type **`telnet 192.11.13.6`**.
2. Login as **`craft`** or **`cust`**.

3. Telnet to the Layer 2 interface.

   Type **`telnet <xxx.xxx.xxx.xxx>`**, where <*xxx.xxx.xxx.xxx*> is the IP address of the G350 interface on the customer's LAN.

4. Login at the Welcome to Avaya G350 CLI screen.

   Login: ***xxx*** *from the planning documentation*
   Password: ***xxx*** *from the planning documentation*

   You are now logged-in at the Supervisor level. The prompt appears as **G350-nnn(super)#**.

   Note:

   To check the syntax of a command in the command line interface, type as much of the command as you know followed by **help**. For example, if you type:
   G350-nnn(super)#> `set help`
   you are given the current list of **`set`** commands available. If you type:
   G350-nnn(super)#> `set interface help`
   you are given a more restricted list of commands that address the possible interfaces to be set.

For a complete list of command line interface commands, type **`help`** or refer to the *Avaya G350 Media Gateway CLI Reference, 555-245-202* (available at http://www.avaya.com/support).

Log in to the G350 interface with a LAN connection

Use this procedure to log in to the G350 interface when you have a connection to the customer's LAN.

To log in to the G350 interface with a LAN connection:

1. With a connection to the customer's LAN (either remotely or on site), telnet to the G350 interface IP address:

   Type **`telnet <xxx.xxx.xxx.xxx>`**, where <*xxx.xxx.xxx.xxx*> is the IP address of the G350 interface on the customer's LAN.

2. Login at the Welcome to Avaya G350 CLI screen.

   Login: ***xxx*** *from the planning documentation*
   Password: ***xxx*** *from the planning documentation*

   You are now logged-in at the Supervisor level. The prompt appears as **G350-nnn(super)#**.

Log in to the G350 interface with a direct Serial connection

Use this procedure to access the G350 interfaces when your laptop is directly connected to the S8300 Console port via a serial cable.

To access the G350 via the Console (serial) port:

1. Launch Windows® HyperTerminal or any other terminal emulation program.

   Note:

   For most Windows-based PCs, you access the HyperTerminal program from the **Start** menu by selecting **Programs**, then **Accessories**.

2. Choose **Call - Connect** (for HyperTerminal) or the appropriate call command for your terminal emulation program.

3. Login at the **Welcome to Avaya G350 CLI** screen.

   Login: xxx *from the planning documentation*
   Password: xxx *from the planning documentation*

   You are now logged-in at the Supervisor level. The prompt appears as **G350-nnn(super)#**.

Log in to the G350 interface with Device Manager

To access the Device Manager, you must have access to the corporate LAN in which the Layer 2 interface resides.

To access the Device Manager

1. Open a compatible Internet browser on your computer. Currently this includes Internet Explorer 5.0 (or higher) and Netscape Navigator 4.7 and 6.2. The Java Plug-in 1.4.2 or higher is required.

2. In the Address (or Location) field of your browser, type the IP address or name of the Layer 2 interface and press Enter.

   - If the network includes a domain name service (DNS) server that has been administered with this IP device's name, you can type the processor's name into the address field instead of the IP address. For example, `http://G350-stack1.mycompany.com`

   Note:

   The Device Manager is *not* available through the S8300 Media Server. You must be connected to the G350 Media Gateway through the corporate LAN.

3. A GUI rendering of the stack devices appears. Proceed with Media Gateway or stack device administration.

Avaya Site Administration

Avaya Site Administration is part of the Avaya VisAbility Suite. Normally, the customer can simply select Download next to the Administration item on the Media Server Home Page to download Avaya Site Administration. The customer then follows the directions presented by the download/installation wizard.

Configure Avaya Site Administration

When Avaya Site Administration is initially installed on a client machine, it must be configured to communicate with Communication Manager on the S8300 Media Server.

When initially running Avaya Site Administration, after downloading, you must create a new entry for the switch connection.

To add an S8300 switch administration item:

1. Click **File** > **New** > **Voice System**.

   The system displays the Add Voice System window.

2. Enter a name in the **Voice System Name:** field. As a technician configuring Avaya site Administration on your laptop, use a generic name, as you will be able to use this connection item for all S8300 Media Servers.

3. Click **Next**.

   The Network Connection/Port Number dialog box appears.

4. **TCP/IP Port Number**: For the port number, use port **23** to login via Linux; use port **5023** to login directly to the Communication Manager CLI screens.

5. Click **Next**.

   The Network Connection/Timeout Parameters dialog box appears. Leave the default values for the timeout parameters.

6. Click **Next**.

   The login type dialog box appears.

7. Click the “**I want to login manually each time**” radio button.

8. Click **Next**.

   The switch summary dialog box appears.

9. Check the information. Use the **Back** button to make corrections, if necessary.

10. Click the **Test** button to test the connection.

11. When the connection is successfully tested, click **Next** and then **Finish**.

Logging in to the S8300 with Avaya Site Administration

To start Avaya Site Administration, click **Start** > **Programs** > **Avaya** > **Site Administration**. Avaya Site Administration supports a terminal emulation mode, which is directly equivalent to the SAT command interface. Avaya Site Administration also supports a range of other features, including the GEDI and Data Import. For more information, refer to Online Help, Guided Tour, and Show Me, accessed from the Avaya Site Administration Help menu.

To use Avaya Site Administration, open the application and select the switch (media server) you want to access. When prompted, log in.

When you are logged in, click **Start GEDI**.

Navigational aid for CLI commands

Table 139: Navigational aid for CLI commands on page 294 describes a few Command Line Interface commands you can use to establish sessions with the media gateway controller or the media server.

Table 139: Navigational aid for CLI commands *1 of 2*

Command	Purpose	Prompt
`session mgc`	open a CLI session on active media gateway controller	
`session icc`	open a CLI session on the S8300 processor	**craft**@<*host name*>**>**
`session mgc sat`	open a CLI session on the active media gateway controller and go to the SAT login	
`session icc sat`	open a CLI session on the S8300 processor and go to the SAT login	
`exit`	close the current session (and revert to the previous session)	

1 of 2

Table 139: Navigational aid for CLI commands *2 of 2*

Command	Purpose	Prompt
<*command*> help	displays help for <*command*>	

2 of 2

The command-line prompts in a G350 CLI session use the media gateway's name that is assigned when it is configured.

You can Telnet to another interface from a current Telnet session.

Terminal emulation function keys for Communication Manager

When you log in to the Communication Manager SAT screens, your terminal emulation may not display function keys on the screen to help you determine which function keys to press. Use Table 140: ntt terminal emulation function keys on page 295 as a guide for **ntt** terminal emulation.

Table 140: ntt terminal emulation function keys

Key Sequence		Function Key	Function
ESC	(alpha O) P	F1	Cancel
ESC	(alpha O) Q	F2	
ESC	(alpha O) R	F3	Execute
ESC	(alpha O) S	F4	
ESC	(alpha O) T	F5	Help
ESC	(alpha O) U	F6	Go to Page "N"
ESC	(alpha O) V	F7	Next Page
ESC	(alpha O) W	F8	Previous Page

Table 141: w2ktt terminal emulation function keys on page 296 lists key presses for **w2ktt** terminal emulation.

Table 141: w2ktt terminal emulation function keys

Key Sequence		Function Key	Function
ESC	x	F1	Cancel
ESC		F2	
ESC	e	F3	Execute
ESC		F4	
ESC	h	F5	Help
ESC		F6	
ESC	n	F7	Next Page
ESC	p	F8	Previous Page

Chapter 6: G350 and Media Module LEDs

LEDs are important status indicators for technicians during on-site installation, maintenance, troubleshooting, and repair. They encompass three major areas: Alarms, Testing, and Usage Activity. Some LEDs are specialized to support specific procedures (such as removing the S8300 Media Server). When alarms or problems occur, LEDs are present to indicate that attention by a technician is needed.

LEDs appear on the G350 front panel, and each Media Module.

Some Media Modules have additional LEDs, although each Media Module has three standard LEDs. Table 142: LED Interpretation on page 297 indicates the meanings associated with standard DEFINITY server LEDs. Although in some cases these LEDs have been augmented or modified for the S8300 Media Server and Avaya G350 Media Gateway, it is important to be aware of their standard meanings when viewing the system.

Table 142: LED Interpretation

Red	Upon power-up or module insanity, this LED is turned on. Upon passing diagnostics, this LED is turned off.
Green	During power-up self testing and maintenance testing, this LED is turned on.
Yellow	This LED indicates that the module is in service.

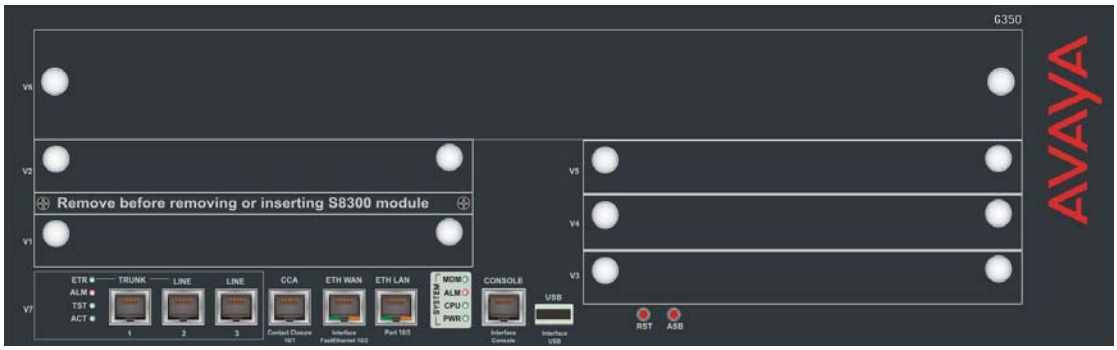
Note:

The four multi-color specialized status LEDs that have appeared on various DEFINITY server TN boards like the T1/E1/DS1 board (TN464F) do not appear on the Media Modules.

G350 front panel LEDs

The following figure shows the G350 chassis:

Figure 16: G350 chassis



System LEDs

The system LEDs show the status of the Avaya G350 Media Gateway. The following table shows the meaning of the system LEDs when they are lit:

Table 143: System LEDs

LED	Name	Color	Meaning
MDM	Modem Detected	Green	A modem is connected to the CONSOLE or USB port
ALM	Alarm	Red	An alarm is present in the system
CPU	CPU	Green	OFF — A test is in progress ON — Normal operation
PWR	Power	Green	OFF — No power BLINKING — Problem with power ON — Normal operation

Analog telephone ports and LEDs

The analog telephone ports are standard RJ-45 telephone network ports.

- TRUNK is a trunk port.
- The two LINE ports are analog telephone ports.

The analog telephone port LEDs show the status of the analog telephone ports.

The following table shows the meaning of the analog telephone LEDs when they are lit:

Table 144: Analog telephone port LEDs

LED	Name	Color	Meaning
ETR	Emergency Transfer	Green	The Emergency Transfer Relay (ETR) feature has been activated. This feature provides an emergency link between the telephone connected to the first LINE port (port 2) and the trunk connected to the TRUNK port if power is disconnected from the G350 or if the G350 becomes unregistered from its Media Gateway Controller (MGC).
ALM	Alarm	Red	An alarm is present on the board
TST	Test	Green	A test is in progress
ACT	Activity	Yellow	A call is in progress

Media Module LEDs

Media Gateway physical LEDs provide the technician with information regarding the ability to troubleshoot the Media Module as a whole.

Note:

The physical LEDs provide board level status information, while the SAT provides port level status information.

LED locations on the Media Modules

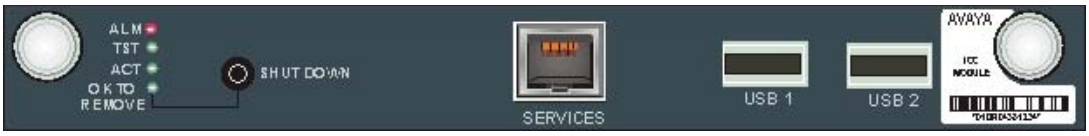
All Media Modules have three standard LEDs on the faceplate (Figure 17: Faceplate of Media Modules with Standard LEDs on page 300). On the Avaya BRI (MM720, MM722), Avaya DCP (MM312, MM712, MM717), Avaya WAN (MM340, MM342), and Avaya Analog (MM711, MM714) Media Modules, these are the only LEDs present. The Avaya T1/E1 Media Module (MM710) has an additional LED, as shown in Figure 18: T1/E1 Media Module with Fourth LED on page 300.

Figure 17: Faceplate of Media Modules with Standard LEDs

Figure 18: T1/E1 Media Module with Fourth LED

S8300 Media Server LEDs

Figure 19: S8300 Media Server



The S8300 Media Server has a total of 4 LEDs on the faceplate (Figure 19: S8300 Media Server on page 301), the three standard LEDs and one additional LED:

- A fourth LED labeled “OK-to-Remove”, which indicates when the S8300’s disk is properly shut down.

GREEN “OK-to-Remove” LED

The S8300 has a hard drive that must be shut down prior to removal of the S8300. Initiate a shutdown process by first depressing the shutdown button located next to the fourth GREEN “Ok-to-Remove” LED for 2-4 seconds (specific to the S8300). The behavior of the S8300’s LEDs during shutdown differs depending on the version of Communication Manager running:

- For Communication Manager versions 1.2 and earlier, the fourth GREEN LED flashes at a constant rate until it finally glows steadily.
- For Communication Manager version 1.3 and later, the fourth GREEN “Ok-to-Remove” LED flashes at a constant rate, and the TST LED flashes slowly at first. As computer processes exit, the TST LED flashes faster. When the shutdown has completed, the TS LED goes out, and the “OK-to-Remove” LED then glows steadily.

Once steady, the GREEN LED indicates that the disk drive has been shut down properly and the S8300 is ready to be removed. Follow standard Media Module removal procedures after the GREEN LED indicates that the disk drive has been properly parked.

There are three different ways that you can properly shut down the S8300 before it is removed:

- Press the shutdown button on the faceplate for 2-4 seconds.
- Initiate shutdown via the Web interface with a computer connected either:
  - Remotely, on the customer’s LAN
  - Locally, on the S8300 using the Services Port on the faceplate of the S8300

S8300 LED differences from Media Modules

Certain behaviors of the traditional S8300 LEDs differ from the Media Modules because the S8300 is a Media Server running Communication Manager.

- Situations like “insanity” and IP concepts of “registered” via H.248 do not necessarily apply to other Media Modules.
- The RED LED provides a major alarm indication. Software turns off the RED LED during system startup. After startup, software turns on the RED LED whenever a major alarm is present, and turns off the RED LED whenever a major alarm clears. Since the S8300 sees a major alarm whenever an Avaya G350 Media Gateway becomes unregistered, this means the RED LED turns on. If the Media Gateway subsequently becomes registered, the major alarm clears, and the RED LED turns off.

  Note:

  For an S8300 configured as an LSP, the converse is true. If an Avaya G350 Media Gateway registers with an LSP, a major alarm is generated, and the RED LED turns on. When the Media Gateway unregisters, the RED LED turns off.

  The RED LED can be turned on by software to report an application or other error. The RED LED can also be turned on by a hardware watchdog that has not been cleared for at least 10ms, when the processing complex has ceased to function.
- The GREEN LED provides self-testing and maintenance indication.
- The YELLOW LED provides active “in use” indication. For an S8300, the software turns on the YELLOW LED during system startup, and turns off the LED during shutdown. During normal call processing operation, the YELLOW LED turns on whenever an Avaya G350 Media Gateway, an IP station, or an IP console is registered with the S8300. Likewise, it turns off when none of the IP endpoints are registered.

Table 145: Major Alarm on page 303 through Table 148: OK to Remove on page 304 illustrate the states of S8300 LEDs.

Table 145: Major Alarm

Major Alarm	
Color	Red
Power On Reset	On
BIOS Boot	On
OS and SW Boot	On
System Up	Off - SW
H.248 Registered	Off - SW
Shutdown in Progress	On
Shutdown Complete	On

Table 146: Test – To Be Defined

Test – To Be Defined	
Color	Green
Power On Reset	Off
BIOS Boot	Off
OS and SW Boot	On-SW
System Up	Off - SW
H.248 Registered	Off - SW
Shutdown in Progress	Off - SW
Shutdown Complete	Off

Table 147: Active – In Use

Active – In Use	
Color	Yellow
Power On Reset	Off
BIOS Boot	Off
OS and SW Boot	Off
System Up	SW
H.248 Registered	On-SW
Shutdown in Progress	Off-SW
Shutdown Complete	Off

Table 148: OK to Remove

OK to Remove	
Color	Green
Power On Reset	Off
BIOS Boot	Off
OS and SW Boot	Off
System Up	Off
H.248 Registered	Off
Shutdown in Progress	1 Hz flash
Shutdown Complete	On

S8300 LED lighting sequence

In general, S8300 LEDs light in order from top to bottom on the S8300 faceplate.

The following order applies during restart or boot of the S8300:

LED Lighting Sequence

1. **ALM - RED** – lights up first then turns off
2. **TST - GREEN** – lights up second then turns off
3. **ACT - YELLOW** – lights up third then turns off
4. **OK To REMOVE - GREEN** – lights up fourth then turns off
5. **ACT - YELLOW** and **OK To REMOVE - GREEN** – light up a second time and then turn off

MM710 T1/E1 Media Module LEDs

The T1/E1 Media Module has four LEDs on its faceplate (see Figure 20: T1/E1 Media Module LEDs on page 306). Table 149: T1/E1 LEDs on page 305 shows their color and functions. The first three are the standard LEDs, which are under software control.

Table 149: T1/E1 LEDs *1 of 2*

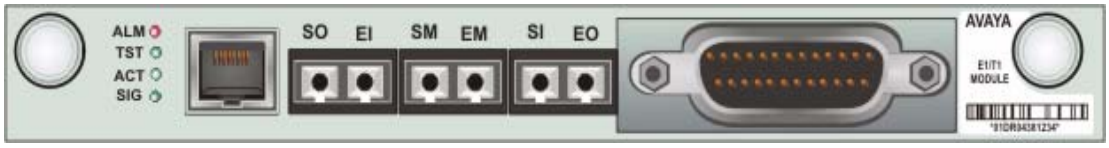
Name	Color	Location	Description
ALM	RED	Top	Upon power-up, this LED is turned on. Upon passing diagnostics this LED is turned off. During normal circuit pack operation this LED is not turned on except for certain alarm states.
TST	GREEN	Second	During power-up self-testing and maintenance testing requested by the SPE, this LED is turned on.

1 of 2

Table 149: T1/E1 LEDs *2 of 2*

Name	Color	Location	Description
ACT	YELLOW	Third	This LED indicates that the clock is synchronized with a source (usually the Central Office). The LED is blinking 2700 ms ON and 300 ms OFF. This is the most common condition. The opposite blinking of the YELLOW LED is 300 ms ON and 2700 ms OFF. This is an error condition, and indicates that the MM710 T1/E1 Media Module is not synchronized with a clock. An infrequent occurrence is a steady YELLOW LED. This indicates in-use activity, only when clock synchronization is set to local.
SIG	GREEN	Bottom	This LED indicates whether the link to the Central Office (CO) is up (equivalent to the TN464F circuit pack Status 3 GREEN LED). See Figure 20: T1/E1 Media Module LEDs on page 306.
			2 of 2

Figure 20: T1/E1 Media Module LEDs



The supported portion of the LED Control message allows software to change the status of the three standard LEDs on the T1/E1 Media Module faceplate. Power-up and alarm states are the only conditions where hardware sets the state of the LEDs independent of ANGEL firmware control. The exceptions to letting software turn off the LEDs are:

- The board is in reset (RED ALM LED remains on)
- A call is up (YELLOW ACT LED remains on while the E1 line is in-frame and at least one voice/data call is up)
- During board reset initialization testing (GREEN TST LED remains on until initialization testing is complete)

Note:

For ISDN operation, the Yellow LED will be turned on if ANY port has an active TDM connection (including the D-channel).

Synchronization

The YELLOW ACT LED on the front of the MM710 Media Module can tell you the status of that module regarding synchronization.

- If the YELLOW ACT LED is solidly on or off, it has NOT been defined as a synchronization source. If it is on, one or more channels is active. If it is an ISDN facility, the D-channel will count as an active channel and will cause the YELLOW ACT LED to be on.
- When the MM710 is driving a clock sync source line to the G350 main clock, the YELLOW ACT LED does not indicate port activity, but instead indicates that the MM710 is the sync source by flashing with a regular 3-second period:
  - It is on for 2.8 seconds and flashes off for 200 milliseconds if it has been specified as a sync source and is receiving a signal that meets minimum requirements for the interface.
  - If it has been specified as a sync source and is not receiving a signal, or is receiving a signal that does not meet minimum requirements for the interface, then the YELLOW ACT LED will be off for 2.8 seconds and flash on for 200 milliseconds.

T1/E1 initialization

The T1/E1 Media Module LEDs behave in the following manner during initialization. The Angel provides a visual indication of the Media Module's status through the three faceplate LEDs:

- During initialization the YELLOW ACT LED is held off, while the RED and GREEN LEDs are on during the entire initialization sequence.
- Upon power up or reset, if only the RED ALM LED comes on, the Angel processor is dead or the board is being held permanently in reset.
- Upon completion of the diagnostics and initialization, the GREEN TST LED turns off.
- If the initialization tests fail, the RED ALM LED remains on.
- If the tests all pass, then all LEDs are extinguished until Communication Manager starts using the Media Module.

Operational control

After successful initialization, the T1/E1 Media Module's LEDs are controlled as follows:

- The Angel lights the YELLOW ACT LED when there is at least one non-idle trunk. If Communication Manager sends a message to drive the clock sync signals, the YELLOW ACT LED indicates this instead of the port busy/idle status.
- The Media Server may independently light and extinguish the three LEDs through downlink LED Control messages, subject to the constraint that it may not turn off a YELLOW ACT LED turned on by the Angel as a result of port activity.
- If the Media Module resets for any reason and is not released from reset, the RED ALM LED lights and the YELLOW ACT and GREEN TST LEDs are held off.

Avaya MM314 Media Module LEDs

The MM314 Media Module is a LAN Media Module that provides:

- 24 Ethernet 10/100 Base-T Ethernet access ports with inline Power over Ethernet (PoE).
- One Gigabit Ethernet 1000 uplink/access port.

Figure 21: The MM314 Media Module front panel

Alarm LED

The MM314's alarm (ALM) LED is located on the lower left corner of the front panel. The ALM LED indicates that an alarm is present in the module, or that Communication Manager (CM) has the slot administered for a Voice Media Module.

Port LEDs

On the left side of the MM314's front panel are numbered LEDs that correspond to each of the MM314's network ports. Underneath these LEDs is a row of LEDs that indicate particular functions. The function LED that is lit indicates which function the network port LEDs are reporting. For example, if the LNK LED is lit, the port LEDs indicate whether the network links for the specific ports are functioning properly.

To the right of the function LEDs are two push buttons. Use these buttons to select the function you want the port LEDs to report. For example, if the COL LED is lit, all the port LEDs are reporting the Collision status of their respective port. The following table shows each of these functions:

LED	Name	Meaning
LNK	Link	If the port LED is lit, the port is enabled and the link is working properly.
COL	Collision	If the port LED is off, there has been no collision on line. If this LED is flashing, there are collisions occurring.
Tx	Transmit to line	If the port LED is lit, data is being transmitted.
Rx	Receive from line	If the port LED is lit, data is being received from the line.
FDX	Half/Full Duplex	If the port LED is lit, the line is operating in Full Duplex mode. If the port LED is off, the line is operating in Half Duplex mode.
FC	Symmetric Flow Control	If the port LED is lit, the port is in Full Duplex and Flow Control mode. If the port LED is off, the port's Flow Control mode is disabled, or the port is operating in Half Duplex mode.
Hspd	High Speed	If the LED is lit, the port is operating at the higher of its possible speeds.
LAG	Link Aggregation Trunking	If the LED is lit, the port belongs to a LAG.
PoE	Power over Ethernet	If the LED is lit, the port is operating in PoE mode.

Chapter 7: Monitoring

The Avaya G350 Media Gateway provides several software tools for monitoring and diagnosing your network. Use these tools to monitor the status of your network operations, and to analyze the flow of information. The tools you can use for monitoring include:

- The packet sniffing service
- The RTP statistics application

Packet sniffing

This section provides information about the G350 packet sniffing service.

Overview

The G350 packet sniffing service allows you to analyze packets that pass through the G350's interfaces. Packets are captured to a buffer based on criteria that you specify. The buffer is then uploaded via FTP to a file that can be analyzed using the Ethereal analysis tool.

The packet sniffing service on the G350 offers several advantages to the network administrator. Since the capture file is saved in the libpcap format, which is the industry standard, it is readable both by the S8300's t-ethereal software, and by standard versions of Ethereal for Unix, Windows, and Linux (see http://www.ethereal.com).

In addition, the G350's packet sniffing service is capable of capturing non-Ethernet packets, such as frame-relay and PPP. Non-Ethernet packets are wrapped in a dummy Ethernet header to allow them to be viewed in a libpcap format. Thus, the G350 allows you to analyze packets on all the interfaces of the device.

The G350's packet sniffing service gives you full control over the memory usage of the sniffer. You can set a maximum limit for the capture buffer size, configure a circular buffer so that older information is overwritten when the buffer fills up, and specify a maximum number of bytes to capture for each packet.

What can be captured

The G350 packet sniffing service captures only the packets handled by the G350 and delivered to the device CPU (“non-promiscuous” mode). This is unlike regular sniffer applications that pick up all traffic on the network.

Streams that can always be captured include:

- H.248 registration
- RTP from the G350
- ARP on the LAN (broadcast)
- All packets that traverse the WAN
- All traffic to/from the G350

Streams that can never be captured because they are switched by the internal Ethernet switch and not by the CPU include:

- H.323 Signaling from an IP phone on the LAN to an ICC on the LAN
- RTP stream between IP phones on the LAN

Streams that can be captured if the G350 is the WAN router include:

- H.323 Signaling from IP phones on the LAN to an ECC over the WAN
- DHCP when the DHCP server is behind the WAN (using the G350 DHCP relay capability)
- RTP stream on an IP phone on the LAN to a remote IP phone

The following sections describe how to configure packet sniffing and analyze the resulting capture file.

Configuring packet sniffing

Packet sniffing configuration consists of the following steps:

1. Enabling packet sniffing
2. Limiting packet sniffing to specific interfaces (if necessary)
3. Creating a capture list that specifies which packets to capture
4. Defining rule criteria for a capture list
5. Viewing the capture list
6. Applying a capture list
7. Configuring packet sniffing settings
8. Starting the packet sniffing service

Enabling packet sniffing

Since the packet sniffing service presents a potential security breach, the administrator must first enable the service on the G350 before a user can start capturing packets. Use the **capture-service** command to enable the packet sniffing service.

Note:

The packet sniffing service can only be enabled by an administrator connecting with a serial cable to the G350 console port.

To disable packet sniffing, use the **no capture-service** command.

Limiting packet sniffing to specific interfaces

By default, the packet sniffing service captures packets and Ethernet frames from all the router's interfaces. You can use the **capture interface** command to limit packet sniffing to a specific interface. For example, use the following command to limit packet sniffing to the Fast Ethernet interface:

```
G350-001(super)# capture interface FastEthernet 10/2
Done!
G350-001(super)#
```

Use the following command to enable packet sniffing on all available interfaces:

```
G350-001(super)# capture interface any
Done!
G350-001(super)#
```

Creating a capture list

By default, the packet sniffing service captures all packets passing through the interfaces on which it is enabled. Use a capture list to selectively filter the packets that are captured by the service.

A capture list contains an ordered list of rules and actions. A rule specifies criteria against which packets are tested. The action tells the G350 whether to capture or not capture packets matching the rule criteria. Only packets that match the specified criteria and have an action of **capture** are captured to the capture file. The rules are evaluated one by one, according to their number. If none of the rules match the packet, the default action is executed. You can set the default action as desired.

Note:

ARP frames are not IP packets and therefore cannot be filtered by capture lists. However, in a healthy network, the ARP frames rate is relatively low.

Use the **ip capture-list** command, followed by the list number, to enter the context of a capture list (and to create the capture list if it does not exist). Capture lists are numbered from 500 to 599. For example:

```
G350-001(super)# ip capture-list 510
G350-001(super-Capture 510)#
```

You can use the following commands to set the parameters of the capture list:

- Use the **cookie** command to set the list cookie for the capture list. This is used by the QoS Manager.
- Use the **name** command to assign a name to the capture list.
- Use the **owner** command to assign an owner to the capture list.
- Use the **ip-rule** command to define rule criteria for the capture list. The following section explains rule criteria in detail.

Defining rule criteria for a capture list

Once in the capture list context, use the **ip-rule** command, followed by a number between 1 and 9999, to define a set of criteria against which to test packets. In addition to the rule criteria, each rule must include a composite operation. The composite operation determines the action the rule takes with respect to packets that match the rule criteria, and can be one of the following:

- capture
- no-capture

For example, the following commands create a rule (rule 10 in capture list 510) that provides that tcp packets are not captured:

```
G350-001(super)# ip capture-list 510
G350-001(super-Capture 510)# ip-rule 10
G350-001(super-Capture 510/ip rule 10)# composite-operation no-capture
Done!
G350-001(super-Capture 510/ip rule 10)# ip-protocol tcp
Done!
G350-001(super-Capture 510/ip rule 10)# composite-operation no-capture
Done!
G350-001(super-Capture 510/ip rule 10)# ip-protocol tcp
Done!
G350-001(super-Capture 510/ip rule 10)#
```

You can use the following rule criteria commands. These commands are described in more detail below.

- **dscp**
- **ip protocol**
- **source ip address**
- **destination ip address**
- **tcp source-port**
- **tcp destination-port**
- **udp source-port**
- **udp destination-port**
- **icmp**

DSCP

Use the **dscp** command, followed by a DSCP value (from 0 to 63) to apply the rule to all packets with the specified DSCP value. For example, the following rule is defined to capture all VoIP Bearer packets (DSCP = 46):

```
G350-001(super)# ip capture-list 520
G350-001(super-Capture 520)# ip-rule 20
G350-001(super-Capture 520/ip rule 20)# composite-operation capture
Done!
G350-001(super-Capture 520/ip rule 20)# dscp 46
Done!
G350-001(super-Capture 520/ip rule 20)#
```

IP protocol

Use the **ip-protocol** command, followed by the name of an IP protocol, to apply the rule to all packets with the specified IP protocol. If you want the rule to apply to all protocols, use **any** after the command (**ip-protocol any**).

For example, the following rule is defined to capture all TCP packets:

```
G350-001(super)# ip capture-list 520
G350-001(super-Capture 520)# ip-rule 20
G350-001(super-Capture 520/ip rule 20)# composite-operation capture
Done!
G350-001(super-Capture 520/ip rule 20)# ip-protocol tcp
Done!
G350-001(super-Capture 520/ip rule 20)#
```

To apply the rule to all protocols except the specified protocol, use the **not** form of this command. For example:

```
G350-001(super-Capture 520/ip rule 20)# not ip-protocol tcp
Done!
G350-001(super-Capture 520/ip rule 20)#
```

Source or destination IP address

Use the **source-ip** command to apply the rule to packets from the specified IP address or range of addresses. Use the **destination-ip** command to apply the rule to packets going to the specified IP address or range of addresses.

The IP range criteria can be any of the following:

- Range. Type two IP addresses to set a range of IP addresses to which the rule applies. You can use wildcards in setting the range. For example:

```
G350-001(super-Capture 520/ip rule 20)# source-ip 135.64.102.0 0.0.255.255
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Single address. Type **host**, followed by an IP address, to set a single IP address to which the rule applies. For example:

```
G350-001(super-Capture 520/ip rule 20)# destination-ip host 135.64.104.102
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Wildcard. Type **host**, followed by an IP address using wildcards, to set a range of IP addresses to which the rule applies. For example:

```
G350-001(super-Capture 520/ip rule 20)# source-ip host 135.0.0.0
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Any. Type **any** to apply the rule to all IP addresses. For example:

```
50-???(super-Capture 520/ip rule 20)# destination-ip any
Done!
G350-001(super-Capture 520/ip rule 20)#
```

To apply the rule to all source or destination IP addresses except the specified address or range of addresses, use the **not** form of the applicable command. For example:

```
G350-001(super-Capture 520/ip rule 20)# not destination-ip 135.64.102.0 0.0.255.255
Done!
G350-001(super-Capture 520/ip rule 20)#
```

Source and destination port range

To specify a range of source and destination ports to which the rule applies, use the following commands, followed by either port name or port number range criteria:

- **`tcp source-port`** — the rule applies to TCP packets from ports that match the defined criteria
- **`tcp destination-port`** — the rule applies to TCP packets to ports that match the defined criteria
- **`udp source-port`** — the rule applies to UDP packets from ports that match the defined criteria
- **`udp destination-port`** — the rule applies to UDP packets to ports that match the defined criteria

The port name or number range criteria can be any of the following:

- Range. Type **`range`**, followed by two port numbers, to set a range of port numbers to which the rule applies. For example:

```
G350-001(super-Capture 520/ip rule 20)# tcp destination-port range 1 3
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Equal. Type **`eq`**, followed by a port name or number, to set a port name or port number to which the rule applies. For example:

```
G350-001(super-Capture 520/ip rule 20)# tcp source-port eq ftp
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Greater than. Type **`gt`**, followed by a port name or port number, to apply the rule to all ports with a name or number greater than the specified name or number. For example:

```
G350-001(super-Capture 520/ip rule 20)# udp destination-port gt 10
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Less than. Type **`lt`**, followed by a port name or port number, to apply the rule to all ports with a name or number less than the specified name or number. For example:

```
G350-001(super-Capture 520/ip rule 20)# udp source-port lt 10
Done!
G350-001(super-Capture 520/ip rule 20)#
```

- Any. Type **`any`** to apply the rule to all port names and port numbers. For example:

```
G350-001(super-Capture 520/ip rule 20)# tcp source-port any
Done!
G350-001(super-Capture 520/ip rule 20)#
```

To apply the rule to all protocols except the specified protocol, use the **not** form of the applicable command. For example:

```
G350-001(super-Capture 520/ip rule 20)# not udp source-port lt 10
Done!
G350-001(super-Capture 520/ip rule 20)#
```

ICMP type and code

To apply the rule to a specific type of ICMP packet, use the **icmp** command. This command specifies an ICMP type and code to which the rule applies. You can specify the ICMP type and code by integer or text string. For example:

```
G350-001(super-Capture 520/ip rule 20)# icmp Echo-Reply
Done!
G350-001(super-Capture 520/ip rule 20)#
```

To apply the rule to all ICMP packets except the specified type and code, use the **not** form of this command. For example:

```
G350-001(super-Capture 520/ip rule 20)# not icmp 1 2
Done!
G350-001(super-Capture 520/ip rule 20)#
```

Capture list example

The following commands create a capture list that captures all traffic from subnet 135.122.50.149 255.255.255.254 to an ECC at address 135.122.50.171, except telnet:

```
G350-001(super)# ip capture-list 511
G350-001(super-Capture 511)# name "list #511"
Done!
! Rules 10 and 15 provide that telnet packets are not captured.
G350-001(super-Capture 511)# ip-rule 10
G350-001(super-Capture 511/ip rule 10)# composite-operation no-capture
Done!
G350-001(super-Capture 511/ip rule 10)# ip-protocol tcp
Done!
! You can use a port number instead of "telenet" (23).
G350-001(super-Capture 511/ip rule 10)# tcp destination-port eq telnet
Done!
G350-001(super-Capture 511/ip rule 10)# exit
G350-001(super-Capture 511)#
G350-001(super-Capture 511)# ip-rule 15
G350-001(super-Capture 511/ip rule 15)# composite-operation no-capture
Done!
G350-001(super-Capture 511/ip rule 15)# ip-protocol tcp
Done!
! You can use a port number instead of "telenet" (23).
G350-001(super-Capture 511/ip rule 15)# tcp source-port eq telnet
Done!
G350-001(super-Capture 511/ip rule 15)# exit
```

```
! Rule 20 provides for capturing any packet coming from the host IP address
! 135.122.50.171 and going to the subnet 135.122.50.128, including packets going
! to any of the 30 possible hosts in that subnet.
G350-001(super-Capture 511)# ip-rule 20
G350-001(super-Capture 511/ip rule 20)# ip-protocol tcp
Done!
G350-001(super-Capture 511/ip rule 20)# source-ip host 135.122.50.171
Done!
G350-001(super-Capture 511/ip rule 20)# destination-ip 135.122.50.128 0.0.0.31
Done!
G350-001(super-Capture 511/ip rule 20)# exit
! Rule 30 provides for capturing any packet coming from the subnet
! 135.122.50.128 and going to the host IP address 135.122.50.171, including
! packets from any of the 30 possible hosts in that subnet.
G350-001(super-Capture 511)# ip-rule 30
G350-001(super-Capture 511/ip rule 30)# source-ip 135.122.50.128 0.0.0.31
Done!
G350-001(super-Capture 511/ip rule 30)# destination-ip host 135.122.50.171
Done!
G350-001(super-Capture 511/ip rule 30)# exit
G350-001(super-Capture 511)# ip-rule default
G350-001(super-Capture 511/ip rule default)# composite-operation no-capture
Done!
G350-001(super-Capture 511/ip rule default)# exit
G350-001(super-Capture 511)# exit
G350-001(super)#
```

Viewing the capture list

Use the **show ip capture-list** command to display the capture list in an easy-to-read format. For example:

```
G350-001> show ip capture-list 511

Index Name                            Owner
----- ------------------------------- -------------------------
511   list #511                        other

Index Protocol     IP               Wildcard        Port         Operation
      DSCP
----- -------- --- ---------------- --------------- ------------ -------------
10     tcp     Src  Any                              Any         No-Capture
       Any     Dst  Any                              eq Telnet

15     tcp     Src  Any                              eq Telnet   No-Capture
       Any     Dst  Any                              Any

20     tcp     Src  135.122.50.171  Host             Any         Capture
       Any     Dst  135.122.50.128  0.0.0.31         Any

30     Any     Src  135.122.50.128  0.0.0.31         Any
       Any     Dst  135.122.50.171  Host             Any

Deflt  Any     Src  Any                              Any         No-Capture
       Any     Dst  Any                              Any


Index Name                 Trust
----- -------------------- ------------
0     Capture              No
1     No-Capture           No
```

Applying a capture list

To apply a capture list, use the **capture filter-group** command from the general context. For example, to set the G350 to use capture list 511 on interfaces in which packet sniffing is enabled, specify the following command:

```
G350-001(super)# capture filter-group 511
Done!
G350-001(super)#
```

If no capture list is applied, the packet sniffing service captures all packets.

Configuring packet sniffing settings

The packet sniffing service provides several administrative settings you can use to control the capture functionality. Use the following commands to configure packet sniffing settings. These commands are all used from general context, and require read/write access.

- Use the **capture buffer-mode** command to specify the type of buffer to use. The available parameters are:
  - ***cyclic***. Circular buffer that overwrites the oldest records when it is filled up. Use a cyclic buffer to store the most recent history of packet activity.
  - ***non-cyclic***. Linear buffer that is used until it is filled up

  For example:

```
G350-001(super)# capture buffer-mode cyclic
Done!
G350-001(super)#
```

- Use the **capture buffer-size** command to specify the maximum size of the capture buffer. Available values are 56 to 10000 kb. The default value is 1000. To activate the change in buffer size, you must run **copy running-config startup-config**, and reboot the G350. For example:

```
G350-001(super)# capture buffer-size 2000
To change capture buffer size, copy the running
configuration to the start-up configuration file, and reset the device.
G350-001(super)# copy running-config startup-config
Beginning copy operation ..................... Done!
G350-001(super)#
```

- Use the **capture max-frame-size** command to specify the maximum number of bytes captured for each packet. This is useful, since in most cases, the packet headers contain the relevant information. Available values are 14 to 1496. The default value is 128. For example:

```
G350-001(super)# capture max-frame-size 4000
This command will clear the capture buffer
 - do you want to continue (Y/N)? y

Done!
G350-001(super)#
```

Note:

When you change the maximum frame size, the G350 clears the capture buffer.

- Use the **clear capture-buffer** command to clear the capture buffer. For example:

```
G350-001(super)# clear capture-buffer
Done!
G350-001(super)#
```

Tip:

To reduce the size of the capture file, use any combination of the following methods:

- Use the **capture interface** command to capture only from a specific interface.
- Use the **capture max-frame-size** to capture only the first N octets of each frame. This is valuable since it is usually the packets headers that contain the interesting information.
- Use capture lists to select specific traffic.

Starting the packet sniffing service

Once you have defined and applied the packet capture lists, use the **capture start** command in general context to instruct the packet sniffing service to start capturing packets.

Note:

The capture start command resets the buffer before starting the sniffer.

Note:

You must apply a capture list using the **capture filter-group** command in order for the capture list to be active. If you do not use the **capture filter-group** command, the packet sniffing service captures all packets.

If packet sniffing has been enabled by the administrator, the following appears:

```
G350-001(super)# capture start
Starting the packet sniffing process
G350-001(super)#
```

If packet sniffing has not been enabled by the administrator, the following appears:

```
G350-001(super)# capture start
Capture service is disable
To enable, use the ‘capture-service‘ command in supervisor mode.
G350-001(super)#
```

Capturing decrypted IPSec VPN packets

IPSec VPN packets are encrypted packets. The contents of encrypted packets cannot be viewed when captured. However, you can use the **capture ipsec decrypted** command to specify that IPSec VPN packets, handled by the internal VPN gateway process, should be captured in clear text format.

Analyzing captured packets

Analyze the captured packets using the following steps:

1. Stop the packet sniffing service.
2. Optionally view information about the packet sniffing service and the captured packets
3. Upload the capture file.
4. Analyze the capture file.

Stopping the packet sniffing service

Use the **capture stop** command to stop the packet sniffing service. You must stop the service in order to upload a capture file.

Note:

The **capture stop** command is not saved in the startup configuration file.

Viewing packet sniffing information

You can use the **show capture** command to view information about the packet sniffing configuration and the capture state. For example:

```
G350-001> show capture

Capture service is enabled and inactive
Capture start time 19/06/2004-13:57:40
Capture stop time 19/06/2004-13:58:23
Current buffer size is 1024 KB
Buffer mode is cyclic
Maximum number of bytes captured from each frame: 1515
Capture list 527 on interface "FastEthernet 10/2"
Number of captured frames in file: 3596 (out of 3596 total captured frames)
Size of capture file: 266 KB (26.6 %)
```

Note:

The number of captured frames can be larger than the number of the frames in the buffer because the capture file may be in cyclic mode.

You can use the **show capture-buffer hex** command to view a hex dump of the captured packets. However, for a proper analysis of the captured packets you should upload the capture file and analyze it using a sniffer application, as described in the following sections.
Following is an example of **show capture-buffer hex** usage:

```
G350-001> show capture-buffer hex
Frame number: 1
Time relative to first frame (D H:M:S:Micro-S): 0, 0:0:0.0
Packet time: 14/01/1970-13:24:55.583598
Frame length: 60 bytes
Capture Length: 60 bytes
00000000:ffff ffff ffff 0040 0da9 4201 0806 0001    .......@..B.....
00000010:0800 0604 0001 0040 0da9 4201 9531 4e7a    .......@..B..1Nz
00000020:0000 0000 0000 9531 4e7a 0000 0000 0000    .......1Nz......
00000030:0000 0000 0000 0000 0000 0000              ............

Frame number: 2
Time relative to first frame (D H:M:S:Micro-S): 0, 0:0:0.76838
Packet time: 14/01/1970-13:24:55.660436
Frame length: 60 bytes
Capture Length: 60 bytes
00000000:ffff ffff ffff 0040 0d8a 5455 0806 0001    .......@..TU....
00000010:0800 0604 0001 0040 0d8a 5455 9531 4e6a    .......@..TU.1Nj
00000020:0000 0000 0000 9531 4e6a 0000 0000 0000    .......1Nj......
00000030:0000 0000 0000 0000 0000 0000              ............
```

Uploading the capture file

Once the packet sniffing service is stopped, upload the capture file to a server for viewing and analysis.

Note:

The capture file may contain sensitive information, such as usernames and passwords of non-encrypted protocols. It is therefore advisable to upload the capture file over a secure channel – via VPN or using SCP (Secure Copy)

In most cases, you can upload the capture file to a remote server. However, in cases where the capture file is very large, or you encounter a WAN problem, you can upload the capture file to an S8300 Media Server and view it using t-ethereal, which is a command-line version of Ethereal.

To upload the capture file to a remote server:

1. Use one of the following commands to upload the capture file:
   - **copy capture-file ftp**
   - **copy capture-file tftp**
   - **copy capture-file scp**

   Note:

   The use of the **copy capture-file scp** command is limited to uploading files of 1 MB or less.

For example:

```
G350-001(super)# copy capture-file ftp myCature.cap 135.64.103.66
This command will stop the capture if capturing is started
Confirmation - do you want to continue (Y/N)? y


Username: xxxx
Password: xxxx
Beginning upload operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show upload status 10' command
G350-001(super)#
```

To upload the capture file to an S8300 server:

1. Telnet into the S8300 server, for example by using the **session mgc** command.
2. Open the Avaya Maintenance Web Interface. For instructions on accessing the Avaya Maintenance Web Interface, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.
3. In the Avaya Maintenance Web Interface, select **FTP** under Security in the main menu.
4. Click **Start Server**.
5. Log into the G350.
6. Use the **copy capture file ftp** command to upload the capture file. Specify that the capture file should be placed in the ftp `'/pub'` subdirectory. For example:

   ```
   G350-001(super)# copy capture-file ftp pub/capfile.cap 149.49.43.96
   ```

7. At the FTP login prompt, enter **anonymous**.
8. At the FTP password prompt, enter your e-mail address.

9. Optionally use the **show upload status 10** command to view upload status. For example:

```
G350-001(super)# show upload status 10
Module #10
==========
Module           : 10
Source file      : sniffer
Destination file : pub/capfile.cap
Host             : 149.49.43.96
Running state    : Executing
Failure display  : (null)
Last warning     : No-warning
```

Analyzing the capture file

The uploaded capture file is in libpcap format and can therefore be viewed by most sniffer applications, including tcpdump, Ethereal and Tethereal.

If you uploaded the capture file to an S3800 server, view the file using Tethereal, a command-line version of Ethereal available on the S3800. See the Tethereal man pages for more information about the Tethereal application.

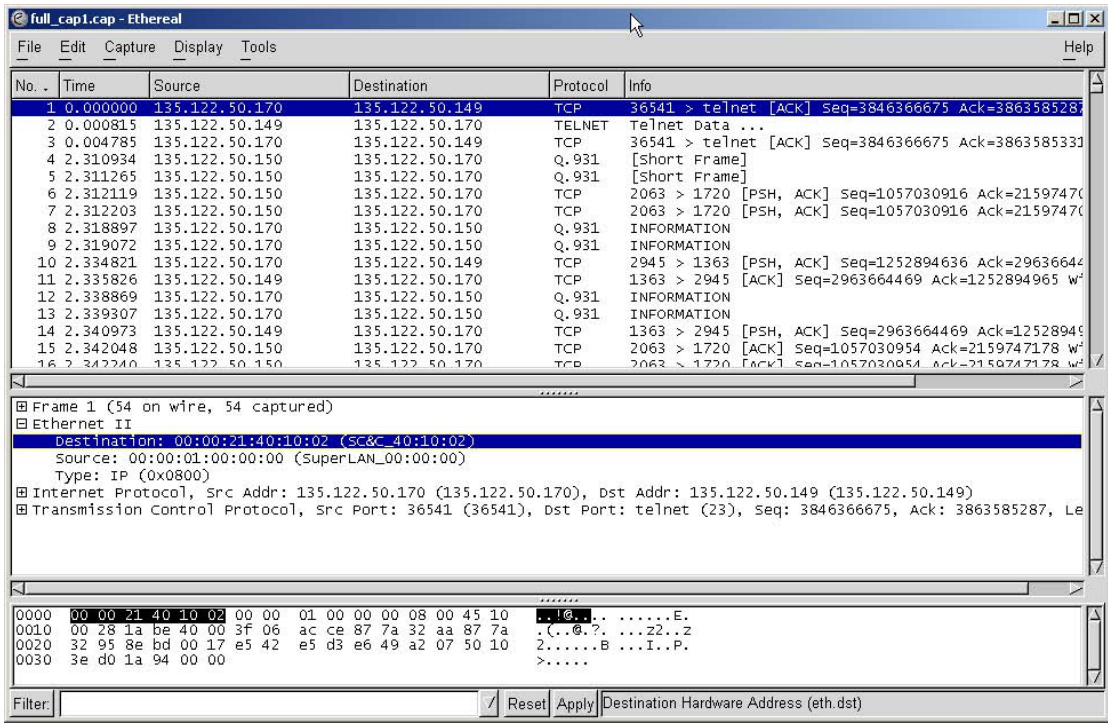
If you uploaded the capture file to a remote server, you can view the file using the industry standard Ethereal application. The latest version of Ethereal for Windows, Linux, UNIX, and other platforms can be downloaded from http://www.ethereal.com.

Note:

Ethereal allows you to create filter expressions to filter the packets in the capture file and display desired files only. For example, you can display only packets with a specific source address, or only those received from a specific interface. See Identifying the interface on page 327.

The following figure shows a sample Ethereal screen.

Figure 22: Sample Ethereal screen



Identifying the interface

The G350's packet sniffing service can capture also non-Ethernet packets, such as frame-relay and PPP, into the capture file. This is achieved by wrapping non-Ethernet packets in a dummy Ethernet header to allow the packets to be stored in a libpcap format. This allows you to analyze packets on all the device interfaces.

The dummy Ethernet headers are allocated according to the original packet type. Dummy Ethernet headers start with 00:00. Therefore if the source or destination address of a packet you are viewing in Ethereal starts with 00:00, this indicates the packet is a non-Ethernet packet. For example, see the highlighted destination address of the packet appearing in the middle pane in Figure 22.

The dummy Ethernet header is identified by special MAC addresses. Packets sent from a non-Ethernet interface are identified with an SA address in the format 00:01:00:00:xx and a DA address which holds the interface index. Packets received over a non-Ethernet interface are identified with DA address in the format 00:01:00:00:xx and an SA address which holds the interface index. The **`show capture-dummy-headers`** command displays the dummy header addresses and their meaning according to the current configuration.

Note:

Ethernet packets received on a VLAN interface are identified by their VLAN tag. However, decrypted IPSec packets received on a VLAN interface are stored with a dummy header.

```
G350-001> show capture-dummy-headers

       MAC                    Description

-----------------  ---------------------------------------------------

00:00:01:00:00:00  Src/dst address of Packet to/from frame-relay or PPP

00:00:01:00:00:01  Decrypted IPSec packet

00:00:0a:00:0a:02  Interface FastEthernet 10/2

00:00:0c:a0:b0:01  Interface Vlan 1

00:00:21:20:10:01  Interface Serial 2/1:1

00:00:21:40:10:02  Interface Serial 4/1:2

00:00:31:00:00:01  Interface Dialer 1
```

Thus in the example appearing in Figure 22:

- The Source address of `00:00:01:00:00:00` indicates that the packet arrived from a frame-relay or PPP interface.
- The Destination address of `00:00:21:40:10:02` indicates that the packet is being sent to the serial interface on the media module in slot number 4, on port number 1, with channel group number 2.

Packet sniffing CLI commands

The following sections list the various packet sniffing CLI commands, by context.

General context

Command	Description	User Level
Capture start	Start capturing packets	R/W
Capture stop	Stop capturing packets	R/W
clear capture buffer	Clear the capture buffer (useful in case it holds sensitive information)	R/W
[no] capture-service	Enable/disable the capture service	Admin
Capture max-frame-size <max-frame-size> **no capture max-frame-size**	Set the maximum octets that are captured from each frame	R/W
Capture filter-group <capture-list-id> **no capture filter-group**	Activate a capture list	R/W
Capture buffer-mode {non-cyclic | cyclic}	Set the capture buffer to cyclic mode	R/W
capture buffer-size <buffer-size-KB> **no capture buffer-size**	Change the size of the capture file	R/W
Capture-e-vlan **no capture-e-vlan**	Enable capture of the internal VLAN	Tech
show capture	Show the sniffer status	R/O
Show capture-buffer hex {<frame-number>}	Show a hex-dump of the captured frames, starting from frame <frame-number>	R/O
ip capture-list <capture-list-id>	Enter the capture list configuration context	R/W
no ip capture-list <capture-list-id>	Delete a capture list	R/W
Show ip capture-list {<capture-list-id>}	Show capture list(s)	R/O
copy capture-buffer {ftp | tftp | scp} <filename> <ip>	Upload the capture buffer to an FTP, TFTP, or SCP server	R/W
Capture interface <ifName> **no capture interface**	Specify a capture interface (by default the service captures from all interfaces simultaneously)	R/W

ip capture-list context

Command	Description	User Level
name <string>	Name a capture list	R/W
ip-rule {<rule-id> | default}	Enter an ip-rule context	R/W
no ip-rule <rule-id>	Erase an ip-rule	R/W
Show list	Show the current list	R/W
Show ip-rule {<rule-id> | default}	Show a specific ip-rule	R/W
Cookie <integer>	Set a number to identify a list (used by the rule-manager application)	R/W
owner <owner-name> **no owner**	Set the name of the person or application that has created the list	R/W

ip-rule context

IP rules are evaluated one by one (according to their number). The composite-operation (`Capture`/`No-capture`) of the first rule to match the packet is executed. If no rule is matched, the **`ip-rule default`** composite-operation is executed.

Note:

The **`not`** operator changes a field operand so it matches when the field does not equal the configured value. Thus, **`not ip-protocol tcp`** specifies all protocols but TCP.

Command	Description	User Level
ip-protocol {<name> | <ip-protocol>} **not ip-protocol**	Set the IP protocol as an operand <ip-protocol> ::= integer (0...255) <name> ::= name of the specific protocol	R/W
source-ip {host <ip-address> | any | <ip-address> <wildcard>} **bi source-ip**	IP protocol operand	R/W
composite-operation {Capture | No-Capture}	The match operation	R/W
		1 of 2

Command	Description	User Level
tcp source-port {any | {eq | lt | gt} {<port-name> | <port-number>} |range <start-port-number> <end-port-number>} not tcp source-port	Set 'ip-protocol' to TCP and an equation on the source port (eq=Equal, lt=Lesser, gt=Greater). The 'not' operator only affects the port section.	R/W
tcp destination-port { any | {eq | lt | gt} {<port-name> | <port-number>} | range <start-port> <end-port> } not tcp destination-port	Set 'ip-protocol' to TCP and an equation on the destination port (eq=Equal, lt=Lesser, gt=Greater). The 'not' operator only affects the port section.	R/W
destination-ip {host <ip-address> | any | <ip-address> <wildcard>} not destination-ip	Define an equation on the destination IP	R/W
udp source-port { any | {eq | lt | gt} { <port-name> | <port-number>} |range <start-port-number> <end-port-number> } not udp source-port	Set 'ip-protocol' to UDP and an equation on the source port (eq=Equal, lt=Lesser, gt=Greater). The 'not' operator only affects the port section.	R/W
udp destination-port { any | {eq | lt | gt} {<port-name> | <port-number>} | range <start-port> <end-port>} not udp destination-port	Set 'ip-protocol' to UDP and an equation on the destination port (eq=Equal, lt=Lesser, gt=Greater). The 'not' operator only affects the port section.	R/W
icmp {<name> | <icmp-type> <icmp-code>} not icmp	Set 'ip-protocol' to ICMP and an equation on the types of ICMP messages. The 'not' operator only affects the ICP message type.	R/W
dscp <dscp> not dscp	Set an equation of the DSCP field	R/W
Show ip-rule [{all | <rule-id>}]	Show the rule	R/W

2 of 2

Ip-rule default context

Command	Description	User Level
composite-operation {capture | No-Capture}	Set the default rule action	R/W
Show ip-rule [{all | <rule-id>}]	Shows the default rule	R/W

Reporting on interface status

You report on the status of an interface using the **show interfaces** command. The command reports on the administrative status of the interface, its operational status, and its extended operational status (the Extended Keepalive status).

For example, if an interface is enabled but normal keepalive packets are failing, show interfaces displays:

```
FastEthernet 10/2 is up, line protocol is down
```

However, if normal keepalive reports that the connection is up but Extended Keepalive fails, the display is:

```
FastEthernet 10/2 is up, line protocol is down (no KeepAlive)
```

The interface status is reported according to the following table:

Table 150: Reporting of Interface Status *1 of 2*

Port Status	Keep-alive status	Show Interfaces Output	Administrative State	Operational State	Extended Operational State
Up	No Keepalive	FastEthernet 10/2 is up, line protocol is up	Up	Up	Up
Up	Keepalive Up	FastEthernet 10/2 is up, line protocol is up	Up	Up	Up
Up	Keepalive down	FastEthernet 10/2 is up, line protocol is down (no KeepAlive)	Up	Up	KeepAlive-Down

1 of 2

Table 150: Reporting of Interface Status *2 of 2*

Port Status	Keep-alive status	Show Interfaces Output	Administrative State	Operational State	Extended Operational State
Down	N/A	FastEthernet 10/2 is up, line protocol is down	Up	Down	FaultDown
Stand by	N/A	FastEthernet 10/2 is in standby mode, line protocol is down	Up	Dormant	DormantDown
Shutd own	N/A	FastEthernet 10/2 is administratively down, line protocol is down	Down	Down	AdminDown
					2 of 2

For detailed specifications of CLI commands, refer to *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

The RTP statistics application

You can use the RTP Statistics application to debug QoS problems across the VoIP network. The RTP Statistics application does not require any dedicated hardware.

For updated information on the RTP Statistics application, see the Avaya web site at http://www.avaya.com/support.

Chapter 8: Alarms

This chapter provides background information on alarming. For detailed information on Avaya G350 Media Gateway Alarming and Media Server Alarming, refer to Chapter 9: G350 traps and Chapter 10: Media Server alarms.

Introduction

During normal operations, software or firmware may detect error conditions pertaining to specific Maintenance Objects (MOs) or other subsystems. The system automatically attempts either to fix or circumvent these problems. Errors are detected in two ways:

- Firmware on the component during ongoing operations
- A “periodic test” or a “scheduled test” started by software

The technician can run tests on demand that are generally more comprehensive (and potentially disruptive) than are the “scheduled tests”.

When an error is detected, the maintenance software puts the error in the Error Log and increments the error counter for that error. When an error counter is “active” (greater than 0), there is a maintenance record for the MO. If a hardware component incurs too many errors, an alarm is raised.

Alarms on the S8300 Media Server with Avaya G350 Media Gateways can occur in several areas:

- Media Modules, Media Servers, and the Media Gateway are all capable of detecting internal failures and generating traps and alarms.
- The G350 detects faults and alerts the Media Server; the Media Server then raises an alarm, and sends the alarm to an appropriate alarm management site.
- Communication Manager alarms reflect G350 health status.
- The Web Interface also displays platform alarms.

Alarms may be viewed using the following:

- Communication Manager Web Interface

  Note:

  For non-Communication Manager alarms, use the Web Page header “Alarms and Notification” and “Diagnostics: View System Log”. Choose the appropriate heading and, if necessary, call Avaya support.

- S8300 SAT CLI
- G350 CLI

Alarm classifications

Alarms are classified depending on their effect on system operation:

- MAJOR alarms identify failures that cause a critical degradation of service. These alarms require immediate attention.
- MINOR alarms identify failures that cause some service degradation but that do not render a crucial portion of the system inoperable. Minor alarms require attention. However, typically a minor alarm affects only a few trunks, stations, or a single feature.
- WARNING alarms identify failures that cause no significant degradation of service or equipment failures external to the switch. These failures are not reported to INADS or to the attendant console.
- ON-BOARD problems originate in the circuitry on the alarmed Media Module.
- OFF-BOARD problems originate in a process or component that is external to the Media Module.

Background terms

Table 151: Alarming Background Terms on page 336 gives a useful explanation of terms.

Table 151: Alarming Background Terms *1 of 2*

Term	Explanation
TRAP	A trap is an event notification that is sent to the SNMP trap manager and received from the Media Gateway, or RTCP Monitor (Avaya VisAbility).
ALARM	Some traps are determined to be an alarm. If determined to be an alarm they are sent to an appropriate alarm management site, such as INADS.
INADS	Initialization and Administration System, a software tool used by Avaya services personnel to initialize, administer, and troubleshoot customer communications systems remotely.
SNMP	Simple Network Management Protocol, the industry standard protocol governing network management and the monitoring of network devices and their functions.
RTCP	Real Time Control Protocol, contained in IETF RFC 1889.

1 of 2

Table 151: Alarming Background Terms *2 of 2*

Term	Explanation
ISM	Intelligent Site Manager, a VPN gateway on the customer's LAN that provides a means for services personnel to access the customer's LAN in a secure manner via the Internet.
VPN	Virtual Private Network, a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
	2 of 2

Alarm-related LEDs

The following alarm-related LEDs appear on the faceplate of the G350 or attendant console, and show how certain LEDs reflect specific alarm situations.

Table 152: Alarm-Related LEDs

LED	Location	Alarm-Related Cause
ALARM LED	Attendant Console	The system alarm causes the attendant console ALARM LED to light.
ACK LED	Attendant Console	The ACK LED on the attendant console reflects the state of acknowledgement of the alarm report from INADS. However, this is only possible for S8700-based Media Servers.
RED ALM or ALARM LED	Front Panel of G350 Media Gateway	The RED ALM or ALARM LED indicates the "health" of the G350 by lighting when there are impaired functions of the Media Gateway. It lights when the power supply voltage is out of bounds, if the G350 cannot locate any Media Servers, or when the unit is overheating. It also indicates that the system is in Power-up mode, or that a Media Module is resetting.

Alarm content

Alarms logged by Communication Manager are stored in an alarm log. All alarms include a date and time stamp that reflects the date and time of the sending device. The alarm contains:

- Device type
- Component type
- Device name
- Current ip address
- Additional information necessary for identification of alarm origination
- Severity level to indicate the priority of the alarm

Alarms originating from an S8300 have a prefix denoting that of an S8300.

QoS alarms

An RTCP monitor using the local SNMP agent generates traps to a pre-administered trap collector. The following alarms are generated:

- The **voip-callqos** alarm is generated if a single session exceeds configured QOS levels. It can generate a warning or an SNMP trap. Warnings are used for less severe problems. They can be accumulated internally within Avaya VoIP Monitoring Manager for use by the alarms defined below.
- The **voip-systemqos** alarm is generated if the number of voip-callqos warnings from all terminals exceeds a configured count over a given period (e.g. 100 alarms over 24 hours). The alarm causes a SNMP trap to be sent.
- The **voip-terminalqos** alarm is like the voip-systemqos alarm except it applies to a single terminal. If any one terminal generates a number of voip-callqos warnings that exceed a threshold then the alarm is generated.

Alarm management

This section describes methods to determine the source of alarms that are generated when an error occurs. The alarm log is viewable and follows that defined in *Maintenance for the Avaya S8700 Media Server with the SCC1 or MCC1 Media Gateway*, 555-233-143. Technicians can view alarms via the Web Interface, CLI, and SAT command-line interface.

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

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

Alarm management for the Avaya G350 Media Gateway follows the S8700 Media Server Alarming Architecture Design; see *Maintenance for the Avaya S8700 Media Server with the SCC1 or MCC1 Media Gateway*, 555-233-143. For convenience, the following sections include some brief information.

Product connect strategies to a services organization

A services organization, such as INADS, receives alarms from the S8300 Media Server running on the Avaya G350 Media Gateway and connects to the product for troubleshooting. There are currently two product-connect strategies: dialup modem access and Virtual Private Network (VPN) access over the Internet.

To connect using dialup modem access:

1. Place a modem connected to a telephone line in front of the Media Server connecting to the USB port on the faceplate.

   You will have to enable the modem from the Web Interface. In addition, there is a Setup Modem Interface under the Configure Server pages. For detailed instructions on enabling the modem, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

2. Via this modem, a client PC uses the Point-to-Point Protocol (PPP) to access the Media Server and connect via telnet to a Linux shell.
3. Once logged into the Media Server, you can telnet out to G350s and other devices on the network.

Note:

Additionally, this modem can be used to allow the Media Server to call out to the INADS or other alarm receiving system to report alarms. When performing remote diagnostic tests, Services personnel should disable alarm call-outs to INADS to avoid generating unnecessary alarms. Alarm suppression is released after 30 minutes. If you are remotely logged in through the modem you prevent alarms from being generated because you are using the modem.

The VPN alternative is achieved via the use of the Intelligent Site Manager (ISM). The ISM is a VPN gateway that resides on the customer's LAN and provides a means for services personnel to gain access to the customer's LAN in a secure manner via the Internet. Telnet is then used to access the Media Server and/or Media Gateways and other IP network equipment.

SNMP alarming on the G350

Setting up SNMP alarm reporting involves two main tasks:

- Configuring the primary media server to report alarms
- Configuring the G350 to send SNMPv3 alarms

Configuring the primary media server to report alarms

The primary server may be either an S8300, S8500, or S8700 Media Server. The Media Server supports two methods for reporting alarms. Either method, both, or no alarm-reporting method may be used at a given site.

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

  To activate OSS alarm notification, the server requires a USB connection to a modem that is connected to an analog line. The modem must be configured using the Web Interface, in 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:

  - Avaya Communication Manager Fault and Performance Manager, as a standalone application, or integrated within Avaya MultiService™ Network Manager
  - HP™ Openview

  Use the Configure Trap Destinations screen on the server Web Interface to set up SNMP destinations in the corporate NMS.

Add INADS Phone Numbers and Enable Alarms to INADS

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

Note:

Perform this task after all Communication Manager administration is complete.

To add INADS phone numbers and enable alarms to INADS:

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

   Note:

   Perform these steps only if the S8300 is the primary controller and the customer has a maintenance contract with Avaya. Use the information acquired from the ART tool. Also, a USB modem must have already been installed.

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

Configuring the G350 to send SNMPv3 alarms

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

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

Configure the host for G350 SNMP traps

Events occurring on the G350 cause SNMP traps to be generated. The G350 Media Gateway can be configured to send SNMP traps to any network management system (NMS) in the network, including the primary server (S8300/S8500/S8700). You specify the destination host using the G350 CLI **`snmp-server host`** command. The traps are sent in User Datagram Protocol (UDP) on the customer's IP network.

The command syntax is:

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

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

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

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

Note:

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

Refer to Table 153: SNMPv3 Notification Types on page 342 for a full list of notification types that can be configured.

Table 153: SNMPv3 Notification Types *1 of 2*

Notification Type	Description
all	All notifications
generic	Generic traps
config	Configuration change notifications
eth-port-faults	Ethernet port fault notifications
sw-redundancy	Software redundancy notifications
temperature	Temperature warning notifications
cam-change	Changes in CAM notifications
l3-faults	L3 level faults (e.g., duplicate IP, VLAN violations)
lag-event	Link aggregation faults and configuration changes
policy	Changes in policy (L3 devices) notifications

1 of 2

Table 153: SNMPv3 Notification Types *2 of 2*

Notification Type	Description
link-down-faults	Link down notifications
supply	Power supply (main and backup) notifications
fan	FAN faults (main and backup) notifications
cascade	Cascade connection fault notifications
	2 of 2

Configure SNMPv3 authentication

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

The G350 provides several pre-configured views and groups for setting up SNMP authentication. Refer to Table 154: G350 Pre-configured Views on page 343 and Table 155: G350 Pre-configured Groups on page 344 for a description of these objects and how they can be used.

Table 154: 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 155: 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
v3AdminViewG	v3 (USM)	3 (AuthPriv)	iso	iso	iso

For a complete discussion of SNMP administration, refer to *Administration of the Avaya G350 Media Gateway*, 555-245-501. For the full syntax of SNMP-related commands and an explanation of their parameters, refer to *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

Chapter 9: G350 traps

A trap indicates a special condition that exists or an event that occurs within the Avaya G350 Media Gateway system. Some traps indicate configuration changes or component modifications and are merely informative. Other traps indicate warning or error conditions that may compromise the performance of the media gateway. Serious traps trigger alarms which are communicated to an alarm management site. For more information about alarms, refer to Chapter 8: Alarms and Chapter 10: Media Server alarms.

This chapter describes the set of traps that are defined for the Avaya G350 Media Gateway.

Alarm format

Avaya G350 Media Gateways (serving either as standalone port networks, or as port networks within a Connect system) report alarms to the primary server (either an S8300, S8500, or S8700 Media Server) using SNMP traps. Like the primary server's own alarms, alarms from an Avaya G350 Media Gateway:

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

However, the format of these displayed alarms is slightly different. Using the G350 MO's Event ID #1 as an example, a displayed G350 alarm has the following format:

```
n CMG 1 WRN 07/17/2002:13:45 121.1.1.2:cmgMultipleFanFault
```

Within the previous alarm-display string, the value:

- "n" is a sequential alarm ID.
- "CMG" identifies an Avaya G350 Media Gateway as the MO.
- "1" is the event's ID.

This table also contains each alarm's corresponding SNMP trap ID in the 2nd column of Table 156: G350 Traps and Resolutions on page 346. However, many of the MIB-defined traps have been excluded, either because:

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

- “WRN” is the event’s severity (5th column of Table 156: G350 Traps and Resolutions on page 346).
- “07/17/2002:13:45” is the event’s date and time stamp.
- “121.1.1.2” is the IP address for Telnet access to the alarmed Avaya G350 Media Gateway Processor (MGP).
- “cmgMultipleFanFault” is the trap name (3rd column of Table 156: G350 Traps and Resolutions on page 346).

G350 traps and resolutions

Although these alarms can be viewed from the primary server, they are normally resolved from within the Avaya G350 Media Gateway. The G350 generates the following traps. Follow the error resolution procedures in Table 156: G350 Traps and Resolutions on page 346 to resolve errors indicated by these traps.

Table 156: G350 Traps and Resolutions *1 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
snmpTraps	1	coldStart	Boot	Warning	The entity is reinitializing itself in such a way as to potentially cause the alteration of either the agent’s configuration or the entity’s implementation. This trap is always enabled.
snmpTraps	2	warmStart	Boot	Warning	The entity is reinitializing itself in such a way as to keep both the agent’s configuration and the entity’s implementation intact. This trap is always enabled.
snmpTrap	3	linkDown	System	Warning	There is a failure in one of the communication links in the agent’s configuration.
snmpTraps	4	linkUp	System	Warning	One of the communication links in the agent’s configuration has come up.
snmpTrap	5	authenticFailure	Security	Notification	The protocol is not properly authenticated.
rmon	1	risingAlarm	Threshold	Warning	An alarm entry has crossed its rising threshold.
rmon	2	fallingAlarm	Threshold	Warning	An alarm entry has crossed its falling threshold.
frame-relay	1	frDLCIStatusChange			A DLCI has been created or deleted, or has state changes.
avayaG350	1	config			The configuration has been changed.

1 of 15

Table 156: G350 Traps and Resolutions *2 of 15*

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

2 of 15

Table 156: G350 Traps and Resolutions *3 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	1	avEntFanFlt	Temp		There is a faulty fan on the device. 1. Verify there are faults in the system. Use the Avaya G350 Media Gateway CLI command show faults to display any faults on the G350. 2. If there is a fan/temperature fault, check to see if the fans are working, and/or if there is sufficient space around the G350 for air circulation. 3. Maintenance software monitors voltages applied to the Media Modules and other components of the 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 G350. Fans and the PSU are not field replaceable.
avEntTraps	2	avEntFanOk	Temp	Notification	A faulty fan has returned to normal functioning.

3 of 15

Table 156: G350 Traps and Resolutions *4 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	4	avEnt48vPwrFlt	Supply		There is a problem with the 48V power supply. 1. Check voltages. Use the CLI command show voltages to determine voltages for Media Modules and other components of the G350. Voltage may be reduced by a short in one of the Media Modules or a bad power supply. 2. Systematically, remove each Media Module to determine if one of the Media Modules is responsible for reducing the voltage levels. Replace faulty Media Module. 3. If the alarm clears in 10-20 seconds, it most likely was a voltage spike. Do not replace the G350. Use a power monitor to monitor the power line. 4. If a brown-out condition is suspected, use a power monitor to monitor the power line. 5. If the fault persists and the show voltages command continues to show the level is out of tolerance, replace the G350.
avEntTraps	7	avEnt5vPwrFlt	Supply		There is a problem with the 5V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	10	avEnt3300mvPwrFlt	Supply		There is a problem with the 3.3V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	13	avEnt2500mvPwrFlt	Supply		There is a problem with the 2.5V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	16	avEnt1800mvPwrFlt	Supply		There is a problem with the 1.8V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	19	avEnt1600mvPwrFlt	Supply		There is a problem with the 1.6V power supply. To resolve the problem, follow the steps for the avEnt48vPwrFlt trap.
avEntTraps	5	avEnt48vPwrFltOk	Supply		The problem with the 48V power supply has been corrected.
avEntTraps	8	avEnt5vPwrFltOk	Supply		The problem with the 5V power supply has been corrected.

4 of 15

Table 156: G350 Traps and Resolutions *5 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	11	avEnt3300mvPwrFltOk	Supply		The problem with the 3.3V power supply has been corrected.
avEntTraps	14	avEnt2500mvPwrFltOk	Supply		The problem with the 2.5V power supply has been corrected.
avEntTraps	17	avEnt1800mvPwrFltOk	Supply		The problem with the 1.8V power supply has been corrected.
avEntTraps	20	avEnt1600mvPwrFltOk	Supply		The problem with the 1.6V power supply has been corrected.
avEntTraps	22	avEntAmbientHiThresholdTempFlt	Temp		The ambient temperature in the device is above the acceptable temperature range. 1. Verify there are faults in the system. Use the Avaya G350 Media Gateway CLI command show faults to display any faults on the G350. 2. If there is a temperature fault, turn off the G350 and allow it to cool. 3. Reboot the G350. Check to see if the fans are working and/or if there is sufficient space around the G350 for air circulation. Use the CLI show faults command to check for fan problems. 4. Low voltage may be responsible for slower fans. Voltage may be reduced by a short in one of the Media Modules or a bad power supply. If there are no fan faults, use the CLI command show voltages to display voltages applied to components on the motherboard and to the Media Modules. 5. If the Media Module voltage is out of tolerance, systematically, remove each Media Module to determine if one of the Media Modules is responsible for reducing the voltage level. If one is found, replace the Media Module. If no Media Module is found to be bad, the power supply is suspect. Replace the G350.
avEntTraps	23	avEntAmbientHiThresholdTempOk	Temp		The ambient temperature in the device has returned to the acceptable range.
avEntTraps	24	avEntAmbientLoThresholdTempFlt	Temp		The ambient temperature in the device is below the acceptable temperature range.

Table 156: G350 Traps and Resolutions *6 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
avEntTraps	25	avEntAmbientLoThresholdTempOk	Temp		The ambient temperature in the device has returned to the acceptable range.
cmgTrapTypes	30	cmgSyncSignalFault		Major	The synchronization signal has been lost. Check that the provisioned clock-sync source has a good signal using the Media Gateway CLI command show sync timing. To set synchronization timing sources on T1/E1 MM or MM710: 1. If the T1/E1 MM has not been added properly on the Media Server, you must use the SAT command ADD DS1 before using the Media Gateway CLI commands set sync interface or set sync source. 2. Specify the primary and secondary clock sources for synchronizing the T1/E1 span, using the CLI command set synch interface. Note: The local clock is "built-in" and not provisionable. 3. Use a set sync source command to set to the specific MM710 T1/E1 Media Module to be used as the active clock reference. 4. Use a show sync timing command to ensure that the source is provisioned and active, or visually inspect the Yellow LED on the MM710 Media Module. Note: When the Yellow LED is on 2.7 seconds and off 0.3 seconds, this means the tone-clock synchronizer is in “active” mode, and an external synchronization source is being used as a synchronization reference. Setting the sync timing was successful. When the Yellow LED is on 0.3 seconds and off 2.7 seconds, this means the tone-clock synchronizer is in “active” mode and the internal (on-board) clock is being used as a synchronization reference. Setting the sync timing was not successful. 5. If there is more than one MM710 Media Module, and they have been set up as primary and secondary, this behavior could be on the second and not the timing of the bus.

Table 156: G350 Traps and Resolutions *7 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	31	cmgSyncSignalClear			The synchronization signal has been regained.
cmgTrapTypes	32	cmgVoipHardwareFault		Major	A DSP complex serving the VoIP engines has failed.
cmgTrapTypes	33	cmgVoipHardwareClear			The DSP complex serving the VoIP engines has returned to normal functioning.
cmgTrapTypes	34	cmgSyncSignalWarn			
cmgTrapTypes	35	cmgSyncWarnClear			
cmgTrapTypes	36	cmgSyncSignalExcess			
cmgTrapTypes	37	cmgSyncExcessClear			
cmgTrapTypes	50	cmgModuleRemove			A Media Module has been removed.
cmgTrapTypes	52	cmgModuleInsertFault			The insertion sequence for a Media Module has failed.
cmgTrapTypes	53	cmgModuleInsertSuccess			A Media Module has been inserted.
cmgTrapTypes	71	cmgFirmwareDownloadSuccess			The Media Gateway successfully downloaded a software or configuration file.
cmgTrapTypes	73	cmgRegistrationSuccess			The Media Gateway has successfully registered with a Media Controller.
cmgTrapTypes	74	cmgMgManualReset			The Media Gateway is beginning a user-requested reset operation.
cmgTrapTypes	75	cmgModuleManualReset			A Media Module is beginning a user-requested reset operation.
cmgTrapTypes	57	cmgDataModuleAwohConflict			

7 of 15

Table 156: G350 Traps and Resolutions *8 of 15*

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

Table 156: G350 Traps and Resolutions *9 of 15*

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

Table 156: G350 Traps and Resolutions *10 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	104	cmgNoControllerFault		Major	The Media Gateway does not have any controllers in its controller list. 1. Verify that the controller list is empty. From the CLI, use the command show mgc list to verify that there are no controllers listed. 2. If none are listed, correct this by adding the correct IP address of the S8700/S8500/S8300. In the CLI's 'configure' mode, use a set mgc list command with the correct IP address.
cmgTrapTypes	105	cmgnoControllerClear			The cmgNoControllerFault trap has been cleared.
cmgTrapTypes	106	cmgRegistrationFault		Major	The Media Gateway cannot register with any controllers in its controller list. 1. Verify that the controller list is correct. From the CLI, use the command show mgc list. The IP address should match the Media Server CLAN or the Media Server IP addresses. 2. If needed, correct this in the CLI's 'configure' mode. Clear the mgc list with the clear mgc list command. Then use a set mgc list with the correct IP addresses. 3. If the IP address in the mgc list matches the Media Server CLAN or the Media Server IP addresses, there may be a network problem. 4. Verify that the primary controller is up.

10 of 15

Table 156: G350 Traps and Resolutions *11 of 15*

Enterprise	Trap ID	Name	Msg Facility	Severity	Description / Resolution
cmgTrapTypes	108	cmgH248LinkDown		Minor	An H.248 link between the Media Gateway and its controller is down. 1. Check the S8300, S8500, or S8700. If down, bring up. 2. If not, check the G350 administration. *Since the following command causes a brief service outage, it should only be executed at the customer's convenience.* 3. If the administration is correct, reboot the G350. 4. If the problem persists, check network connectivity. Use ping or traceroute to the S8300/S8500/ S8700 to check connectivity. 5. If the problem persists, speak to an Avaya technical professional.
cmgTrapTypes	109	cmgH248LinkUp			An H.248 link between the Media Gateway and its controller that was down has come back up.

11 of 15

Table 156: G350 Traps and Resolutions *12 of 15*

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

12 of 15

Table 156: G350 Traps and Resolutions *13 of 15*

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

13 of 15

Table 156: G350 Traps and Resolutions *14 of 15*

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

14 of 15

Table 156: G350 Traps and Resolutions *15 of 15*

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

15 of 15

Chapter 10: Media Server alarms

In the Avaya S8300 Media Server with an Avaya G350 Media Gateway system, some maintenance processes take place on the G350 while others are controlled by Avaya Communication Manager and pertain to the S8300.

Table 160: Alarm #8 on page 365 through Table 193: Alarm #65 on page 382 include selected Communication Manager Media Server alarms. They may come from either an S8300, S8500, or S8700 Media Server.

Note:

For additional Media Server alarm information, refer to *Maintenance for the Avaya S8700 Media Server with the SCC1 or MCC1 Media Gateway*, 555-233-143.

Media Server alarms

A Linux-based Media Server (internal or external) is configured so that it serves as the trap collector and provides external alarm notification.

A process called the Global Maintenance Manager (GMM) runs on the Media Server and collects events that are logged to the Linux syslog_d process. These events consist primarily of failure notification events logged by Communication Manager and INTUITY maintenance subsystems. For events that require external notification, the most basic choice is to call the Avaya technical service center's INADS (Initialization and Administration System). However, other possible methods are sending an e-mail and/or page to specified destinations and sending an SNMP trap to a specified network management station.

The Media Server also has an SNMP trap manager that collects traps from:

- Uploads and downloads to the Media Modules
- VoIP internal Media Module
- VoIP engine on the motherboard
- G350-associated UPS system

Viewing the alarm

The technician views alarms and events through the commands in Table 157: Commands for Viewing Alarms on page 362, which are available via the Web Interface and SAT command-line interface.

Table 157: Commands for Viewing Alarms

Command	Interface	Purpose	Description
View Current Alarms	Web Interface, under Alarms and Notification	To view a list of outstanding alarms against Communication Manager	Displays a summary of alarms (if present), followed by a detailed table of explanation.
display alarms	SAT CLI	To view logged Communication Manager alarms	These are the alarms that have not yet been cleared, either manually or via an Expert System.

Alarming on the Avaya S8300 Media Server

S8300 alarms can be tested and corrected using SAT commands or the Web interface. If you run the Communication Manager application either from a Telnet session (SAT window) or Avaya Site Administration, you can use the following SAT commands to obtain more information.

To obtain information from Communication Manager alarms:

1. Use **`display alarms`** command:

   Issuing the **`display alarms`** command at the administration terminal shows where maintenance software has logged alarms. The alarms are a good indication of the cause of system problems. They should be used in combination with the following.

2. Observe RED LEDs on the Media Modules to determine if software or firmware had a problem.
3. Use the **`reset`** command.

Clear Communication Manager alarms with various SAT commands and corrective actions documented in *Maintenance for Avaya DEFINITY® Server R*, 555-233-117.

CAUTION:

Only trained Avaya technicians should clear alarms.

Alarming on an external Media Server

Alarms for external media servers follows that described for the S8700 or DEFINITY servers. See *Maintenance for the Avaya S8700 Media Server with the SCC1 or MCC1 Media Gateway*, 555-233-143 or *Maintenance for Avaya DEFINITY® Server R*, 555-233-117.

Alarming on the S8300 functioning as a Local Survivable Processor

The S8300 functioning as a Local Survivable Processor (LSP) logs an alarm when it becomes active. It also logs an alarm for every G350 Media Gateway that registers with it. It does NOT log alarms when IP phones register with it; rather, it logs a warning.

Communication Manager alarms

The following sections address Communication Manager alarms for internal and external configurations.

Communication Manager hardware traps

Table 158: Communication Manager Hardware S8300 Traps on page 363 illustrates hardware traps that apply to Communication Manager on the S8300.

Table 158: Communication Manager Hardware S8300 Traps

Trap	Description
Media Server HW trap	Hardware faults are analyzed by maintenance software and correlate fault conditions to determine the appropriate action. If appropriate action requires attention, a trap of critical severity is sent.
Media Server HW clear trap	Hardware faults that have created traps send a clear trap upon clearing.
Media Server with administered MG that is not registered	If a Media Server has an administered G350 but it has not registered after an appropriate amount of time, send an alarm of major severity indicating such.

Note:

The Avaya S8300 Media Server with a G350 Media Gateway platform has several watchdog timers. If any one of them is not verified regularly, a trap of major severity is sent. The timer associated with the S8300 is the S8300 Software watchdog, which resets the S8300 processor if its connection is not verified regularly.

Backup and restore traps

The S8300 uses the LAN to backup a copy of its translation data. Table 159: Backup and Restore Traps on page 364 illustrates the backup and restore traps.

Table 159: Backup and Restore Traps

Trap	Description
successfully stored backup	A trap of informational severity is sent when backup is successful. (REPLY_ACK) The trap reads “Successful backup of S8300 translation data,” and names the backup location stored in the string “BACKUP_LOCATION.” This information also goes to the local maintenance screen, since it is very possible that a backup is being requested as a result of an on-site attempt to replace the S8300.
no backup data stored	A trap of major severity is sent as soon as a REPLY_ERROR message is returned. The trap states “Translation Data backup not available,” and names the backup location stored in the string “BACKUP_LOCATION.”

S8300 alarms – _WD

See Table 160: Alarm #8 on page 365 through Table 169: Alarm #17 on page 370 for a list of S8300 Alarms – _WD.

Table 160: Alarm #8

Number	8
Source	_WD
Event ID	4
Alarm Level	Major
Alarm Text Description	Maximum retries for app start
Possible Causes	Application failed (cannot start) maximum allowed number of times. The application is present but not launching.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	1. On the Web Interface, choose View Process Status and select the appropriate settings 2. From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

Table 161: Alarm #9 ***1 of 2***

Number	9
Source	_WD
Event ID	6
Alarm Level	Major
Alarm Text Description	Cannot open config parameter file
Possible Causes	Watchdog cannot read its configuration file /etc/opt/ecs/watchd.conf

1 of 2

Table 161: Alarm #9 *2 of 2*

Number	9
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	1. Get a fresh copy of watchd.conf (from the CD for field, and from remote server or /root2 for the labs). 2. From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear
	2 of 2

Table 162: Alarm #10

Number	10
Source	_WD
Event ID	7
Alarm Level	Major
Alarm Text Description	Cannot open exe using config file PID
Possible Causes	Watchdog has a bad path name for an application it is supposed to start.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	1. Verify that the file named in the log exists and is executable. 2. Verify that the string in watchd.conf is correct. 3. From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

Table 163: Alarm #11

Number	11
Source	_WD
Event ID	15
Alarm Level	Major
Alarm Text Description	Detected a rolling reboot
Possible Causes	Watchdog has detected x number of Linux reboots within y minutes, where x and y are configurable in /etc/opt/ecs/watchd.conf. A variety of bad things could have happened to cause a rolling reboot, it's not possible to list them all.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	1. (Lab only) Make sure all the executables listed in the watchd.conf exist and are executable. It has been found that the most common cause for rolling reboot is that files are not where they are expected 2. If everything looks OK with step 1, further investigation of trace log is necessary.

Table 164: Alarm #12

Number	12
Source	_WD
Event ID	18
Alarm Level	Warning
Alarm Text Description	Application Restarted
Possible Causes	An application has failed and watchdog has restarted it successfully.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

Table 165: Alarm #13

Number	13
Source	_WD
Event ID	19
Alarm Level	Minor
Alarm Text Description	Application failed unintentionally
Possible Causes	Watchdog is bringing the system down because an application has failed to start correctly. The application may have failed to start because the file did not exist (coincident with 7), or required parameters for the application in watchd.conf were missing or invalid.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	1. Verify that the file named in the log exists and is executable. 2. Verify that the string in watchd.conf is correct. 3. From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

Table 166: Alarm #14

Number	14
Source	_WD
Event ID	20
Alarm Level	Major
Alarm Text Description	Application totally failed
Possible Causes	Application failed maximum allowed number of times.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	1. Access the web page; view summary status 2. If the application is down, use “start -s application” to start the application. 3. From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

Table 167: Alarm #15

Number	15
Source	_WD
Event ID	22
Alarm Level	Minor
Alarm Text Description	Application was shutdown
Possible Causes	Watchdog successfully shut down the named application
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

Table 168: Alarm #16

Number	16
Source	_WD
Event ID	23
Alarm Level	Major
Alarm Text Description	Watchd high monitor thread is rebooting the system
Possible Causes	The lo-monitor thread is missing heartbeats (can't get CPU time) and the hi-monitor thread has tried 3 times to recover the system by killing processes in an infinite loop. That is, if after 3 CPU occupancy profiles and recovery the lo-monitor thread is still not heartbeating, then watchd reboots the server.
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	Clear alarm: From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear. Watch to see if alarm returns. The server should have rebooted by the time a support person can analyze the system. A reboot normally fixes problems with unresponsive software.

Table 169: Alarm #17

Number	17
Source	_WD
Event ID	24
Alarm Level	Major
Alarm Text Description	Watchd high monitor thread is stopping tickling of hw
Possible Causes	This alarm is generated if rebooting the server for alarm 23 does not work. This reboot is done through a Linux system call which may not succeed. This can occur if Linux kernel semaphore is stuck. watchd starts a timer prior to calling reboot. If the timer expires, watchd will stop the HW sanity tickling in hope that the HW sanity watchdog will reboot the processor (i.e. a hard reboot).
Determining Cause	Go to the Web Interface; choose Diagnostics; View System Logs; select Watchdog Logs
Resolution	Clear alarm: From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear. Watch to see if alarm returns. The server should have rebooted by the time a support person can analyze the system. A reboot normally fixes problems with unresponsive software.

S8300 alarms – ENV

See Table 170: Alarm #22 on page 371 for a list of S8300 Alarms – ENV.

Table 170: Alarm #22

Number	22
Source	ENV
Event ID	4
Alarm Level	Major
Alarm Text Description	Temperature reached Critical High
Possible Causes	Motherboard's Temperature reached Critical High
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	1) look for any obstructions blocking the G350 fans 2) check for G350 fan alarms 3) clear alarms 4) shutdown 5) restart 6) If the alarm condition is not present, use “almclear -n #id” to manually clear the alarm. 7) From the Web Interface, choose Alarms and Notification; select the appropriate alarm; choose Clear

S8300 alarms – login

See Table 171: Alarm #44 on page 372 through Table 175: Alarm #48 on page 373 for a list of S8300 Alarms – login.

Table 171: Alarm #44

Number	44
Source	login
Event ID	1
Alarm Level	Warning
Alarm Text Description	
Possible Causes	
Determining Cause	Choose View Current Alarms
Resolution	Notify Customer

Table 172: Alarm #45

Number	45
Source	login
Event ID	2
Alarm Level	Warning
Alarm Text Description	
Possible Causes	
Determining Cause	Choose View Current Alarms
Resolution	Notify Customer

Table 173: Alarm #46

Number	46
Source	login
Event ID	3
Alarm Level	Minor
Alarm Text Description	
Possible Causes	Security violation
Determining Cause	Choose View Current Alarms
Resolution	Notify customer

Table 174: Alarm #47

Number	47
Source	login
Event ID	4
Alarm Level	Minor
Alarm Text Description	
Possible Causes	Security violation
Determining Cause	Choose View Current Alarms
Resolution	Notify customer

Table 175: Alarm #48

Number	48
Source	login
Event ID	5
Alarm Level	Major
Alarm Text Description	
Possible Causes	Security violation
Determining Cause	Choose View Current Alarms
Resolution	Notify customer

S8300 alarms – _TM

See Table 176: Alarm #48 on page 374 for a list of S8300 Alarms – _TM.

Table 176: Alarm #48

Number	18
Source	_TM
Event ID	1
Alarm Level	Major
Alarm Text Description	Can not read translations
Possible Causes	Disk failure or software failure.
Determining Cause	Choose View Current Alarms
Resolution	1. Backup translations to a unique location (for possible later diagnostic use) 2. Restore most recent previous translations. 3. Restart Communication Manager (reset system 4). 4. Notify Tier 3.

S8300 alarms – UPS

See Table 177: Alarm #49 on page 375 through Table 193: Alarm #65 on page 382 for a list of S8300 Alarms – UPS.

Table 177: Alarm #49

Number	49
Source	UPS
Event ID	1-8
Alarm Level	Major (SUP)
Alarm Text Description	upsEstimatedMinutesRemaining
Possible Causes	UPS does not have AC power source
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Return AC power to UPS

Table 178: Alarm #50

Number	50
Source	UPS
Event ID	12
Alarm Level	Major
Alarm Text Description	upsAlarmShutdownPending
Possible Causes	A shutdown-after-delay countdown is underway -- i.e., the UPS has been commanded off
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	

Table 179: Alarm #51

Number	51
Source	UPS
Event ID	13
Alarm Level	Major
Alarm Text Description	upsAlarmShutdownImminent
Possible Causes	UPS will turn off power to the load in less than 5 seconds
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Return AC power to UPS

Table 180: Alarm #52

Number	52
Source	UPS
Event ID	14
Alarm Level	Major
Alarm Text Description	upsAlarmDepletedBattery
Possible Causes	The UPS will be unable to sustain the present load when and if the utility power is lost
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Batteries need to be charged or replaced

Table 181: Alarm #53 ***1 of 2***

Number	53
Source	UPS
Event ID	15
Alarm Level	Major

1 of 2

Table 181: Alarm #53 *2 of 2*

Number	53
Alarm Text Description	upsAlarmBatteryBad
Possible Causes	One or more batteries needs to be replaced
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Replace battery(ies)
	2 of 2

Table 182: Alarm #54

Number	54
Source	UPS
Event ID	16
Alarm Level	Minor
Alarm Text Description	upsAlarmInputBad
Possible Causes	An input condition is out of tolerance
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	provide appropriate AC power to the UPS

Table 183: Alarm #55 *1 of 2*

Number	55
Source	UPS
Event ID	17
Alarm Level	Minor
Alarm Text Description	upsAlarmTempBad
Possible Causes	A temperature is out of tolerance.
	1 of 2

Table 183: Alarm #55 ***2 of 2***

Number	55
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Change environment temperature (increase or decrease depending on which has occurred) or change alarming thresholds

2 of 2

Table 184: Alarm #56

Number	56
Source	UPS
Event ID	18
Alarm Level	Minor
Alarm Text Description	upsAlarmCommunicationsLost
Possible Causes	A problem has been encountered in the communications between the agent and the UPS.
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Requires diagnosing the UPS – may be simpler to just replace it and diagnose it later

Table 185: Alarm #57

Number	57
Source	UPS
Event ID	19
Alarm Level	Warning
Alarm Text Description	upsAlarmBypassBad
Possible Causes	bypass is out of tolerance
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	return AC input power to UPS

Table 186: Alarm #58

Number	58
Source	UPS
Event ID	20
Alarm Level	Warning
Alarm Text Description	upsAlarmLowBattery
Possible Causes	Remaining battery run-time is less than or equal to specified threshold
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Return AC input power to UPS

Table 187: Alarm #59

Number	59
Source	UPS
Event ID	21
Alarm Level	Warning
Alarm Text Description	upsAlarmUpsOutputOff
Possible Causes	UPS has shutdown output power as requested
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Turn-on output power – can be done via SNMP messages

Table 188: Alarm #60 ***1 of 2***

Number	60
Source	UPS
Event ID	22
Alarm Level	Warning

1 of 2

Table 188: Alarm #60 *2 of 2*

Number	60
Alarm Text Description	upsAlarmOutputBad
Possible Causes	Output on one of the receptacles is out of tolerance
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Requires diagnosing the UPS – may be simpler to just replace it and diagnose it later
	2 of 2

Table 189: Alarm #61

Number	61
Source	UPS
Event ID	23
Alarm Level	Warning
Alarm Text Description	upsAlarmOutputOverload
Possible Causes	Load on the UPS exceeds its output capacity
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Reduce the load on the UPS

Table 190: Alarm #62 *1 of 2*

Number	62
Source	UPS
Event ID	24
Alarm Level	Warning
Alarm Text Description	upsAlarmChargerFailed
Possible Causes	UPS charger has failed
	1 of 2

Table 190: Alarm #62 *2 of 2*

Number	62
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Requires diagnosing the UPS -- may be simpler to just replace it and diagnose it later

2 of 2

Table 191: Alarm #63

Number	63
Source	UPS
Event ID	25
Alarm Level	Warning
Alarm Text Description	upsAlarmFanFailure
Possible Causes	One or more UPS fans have failed
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Fix fan

Table 192: Alarm #64

Number	64
Source	UPS
Event ID	26
Alarm Level	Warning
Alarm Text Description	upsAlarmFuseFailure
Possible Causes	One or more UPS fuses have failed
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Replace fuse

Table 193: Alarm #65

Number	65
Source	UPS
Event ID	27
Alarm Level	Warning
Alarm Text Description	upsAlarmGeneralFault
Possible Causes	General fault in the UPS has occurred
Determining Cause	Alarm condition present indicates the problem occurred.
Resolution	Requires diagnosing the UPS – may be simpler to just replace it and diagnose it later

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X