# Maintenance Procedures

555-245-103
Issue 1.1
December 2003

### 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.

### 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 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

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 operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

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
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

**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.

**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). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

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

This document provides procedures to monitor, test, and maintain an Avaya Media Server or Gateway system. It covers many of the faults and troubles that can occur and provides simple procedures to correct them. Simple, traditional troubleshooting methods are sometimes sufficient to locate and clear faults. The traditional methods include substitution, visual inspections, continuity checks, and clarification of operating procedures with end users.

Using this documentation, the Avaya technicians and the technicians of their business partners and customers should be able to follow detailed procedures for:

- Monitoring, testing, and maintaining an Avaya Media Server, Media Gateway, and many other system components.
- Using troubleshooting methods to clear faults.
- Required replacements, visual inspections, continuity checks, and clarifying operating procedures with end users.

## Audience

The information in this book is intended for use by:

Avaya technicians, provisioning specialists, business partners, and customers, specifically:

- Trained Avaya technicians
- A maintenance technician dispatched to a customer site in response to a trouble alarm or a user trouble report
- A maintenance technician located at a remote maintenance facility
- The customer’s assigned maintenance technician

  The technician is expected to have a knowledge of telecommunications fundamentals and of the particular Avaya Media Server and/or Media Gateway to the extent that the procedures in this book can be performed, in most cases, without assistance.

This book is not intended to solve all levels of troubles. It is limited to troubles that can be solved using:

- The Alarm Log
- The Error Log
- Trouble-clearing procedures
- Maintenance tests
- Traditional troubleshooting methods

If the trouble still has not been resolved, it is the maintenance technician’s responsibility to escalate the problem to a higher level of technical support. Escalation should conform to the procedures in the Technical and Administration Escalation Plan.

# Downloading this book and updates from the Web

You can download the latest version of this book *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://support.avaya.com.
2. At the top center of the page, click **Product Documentation**.

   The system displays the Welcome to Product Documentation page.
3. In the upper-left corner type the 9-digit book number in the Search Support field**,** and then click **Go**.

   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 in zipped PDF format

# Safety and security-alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

**CAUTION:**
A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

**WARNING:**
A warning statement calls attention to a situation that can result in harm to hardware or equipment.

**DANGER:**
**A danger statement calls attention to a situation that can result in harm to personnel.**

**SECURITY ALERT:**
A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system or access to network resources.

# Safety precautions

When performing maintenance or translation procedures on the system, users must observe certain precautions. Observe all caution, warning, and danger admonishments to prevent loss of service, possible equipment damage, and possible personal injury. In addition, the following precautions regarding electromagnetic interference (EMI) and static electricity must be observed:

## Electromagnetic interference

This equipment generates, uses, and can radiate radio frequency energy. Electromagnetic fields radiating from the switch may cause noise in the customer's equipment. If the equipment is not installed and used in accordance with the instruction book, radio interference may result.

**WARNING:**
To maintain the EMI integrity of the system, maintenance personnel must ensure that all cabinet doors, panels, covers, and so forth, are firmly secured before leaving the customer's premises.

# Related resources

Table 1, Additional document resources, on page 17 lists additional documentation that is available for you, and which has been referenced within this document.

**Table 1: Additional document resources**

| Document | Number |
|---|---|
| Hardware Guide for Avaya Communication Manager, 555-233-200 | 555-233-200 |
| Administrator's Guide for Avaya Communication Manager, 555-233-506 | 555-233-506 |
| Overview for Avaya Communication Manager, 555-233-767 | 555-233-767 |
| Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server, 555-234-100 | 555-234-100 |
| Administration for Network Connectivity for Avaya Communication Manager, 555-233-504 | 555-233-504 |
| Avaya P330 Manager User Guide | N/A |
| Avaya P333T User's Guide | N/A |
| Getting Started with the Avaya S8700 Media Server with the Avaya G650 Media Gateway, 555-245-703 | 555-245-703 |

*(1 of 2)*

**Table 1: Additional document resources**

| Document | Number |
|---|---|
| Installing the Avaya S8700 Media Server with an Avaya G650 Media Gateway, 555-245-109 | 555-245-109 |
| Installing the S8500 Media Server with the G650 Media Gateway, 555-245-107 | 555-245-107 |
| Overview for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateway, 555-233-231 | 555-233-231 |
| Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146 | 555-233-146 |
| 4606 IP Telephone User's Guide, 555-233-775 | 555-233-775 |
| 4624 IP Telephone User's Guide, 555-233-776 | 555-233-776 |
| 4612 IP Telephone User's Guide, 555-233-777 | 555-233-777 |
| Job Aid: Replacing the S8500 Hard Drive, 555-245-761 | 555-245-761 |
| Job Aid: Replacing the S8500 Media Server, 555-245-762 | 555-245-762 |
| Job Aid: Replacing the G700 Media Gateway, 555-245-752 | 555-245-752 |
| | ***(2 of 2)*** |

# Technical assistance

Avaya provides the following resources for technical assistance.

## Within the United States

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 Avenue
  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.

# How to use this document

Most maintenance sessions involve analyzing the Alarm and Error Logs to diagnose a trouble source and replacing a component such as a circuit pack or media module. The information in the *Maintenance Alarms Reference (555-245-102)* generally addresses these needs. Certain complex elements of the system require a more comprehensive approach. Special procedures for these elements appear in Chapter 6, “Troubleshooting”.

**NOTE:**
This document is designed to be read online and in paper format. Because of the large volume of information, additional cross-references have been added to make it easier to locate information when using the manual online.

## Organization

This Maintenance Procedures volume contains these chapters:

- Chapter 1, “Maintenance strategy”, describes the system’s design and maintenance strategy.
- Chapter 2, “Access and login procedures”, discusses the various means of connecting to and logging in to Avaya equipment.
- Chapter 3, “License and Authentication files”, describes the License and Authentication File functions and how to obtain and install a License or Authentication file.

- Chapter 4, “Hardware configurations”, shows the locations and arrangements of the system’s cabinets, carriers, circuit packs, and cabling.
- Chapter 5, “Server initialization, recovery, and resets”, describes the various reset and reboot processes and how these are used to perform maintenance and recover systems or subsystems that are out of service. Use of the terminal SPE-down interface on non-functional or standby Switch Processor Elements is included here.
- Chapter 6, “Troubleshooting”, describes general repair procedures such as replacing circuit packs and special troubleshooting procedures such as those for fiber link and packet bus faults.
- Chapter 7, “Packet and serial bus maintenance”, describes fault isolation and repair procedures for the packet bus and the G650 serial bus.
- Chapter 8, “Component replacement”, describes preventive maintenance, procedures for replacing fans, filters, hard drives, servers, and interfaces.
- Chapter 9, “Additional maintenance procedures”, describes component, trunk, and feature testing; removing and restoring power to servers, gateways, and IP endpoints; Automatic Transmission Measurement System (ATMS) tests and analyses; and other procedures not associated with specific alarms or components.

# Conventions used in this document

Table 2, Typography used in this book, on page 20 lists the typographic conventions in this document.

**Table 2: Typography used in this book**

| To represent... | This typeface and syntax are shown as... | For example... |
|---|---|---|
| Specific component information | • Avaya component model number<br>• Indented lines set apart extended information intended for a specific system component. | **S8700**: Ensure that the duplication link is securely connected.<br><br>**G650**<br><br>Ensure that Media Module is securely seated and latched in the carrier. |
| SAT commands | • Bold for **commands**<br>• Bold italic for ***variables***<br>• Square brackets **[ ]** around optional parameters<br>• “\|” between exclusive choices | **refresh ip-route [all \| *location*]** |

***(1 of 2)***

**Table 2: Typography used in this book**

| To represent... | This typeface and syntax are shown as... | For example... |
|---|---|---|
| SAT screen input and output | • Bold for **input**<br>• Constant width for `field names and output (screen displays and messages)` | Set the `Save Translation` field to **daily**.<br>The message `Command successfully completed` appears. |
| Linux commands | • Constant-width bold for **`system-generated information`**.<br>• Constant-width bold italics for ***`variables`***<br>• Square brackets **`[]`** around optional arguments<br>• "Or" sign **`\|`** between exclusive choices | **`testmodem [-s] \| [-t arg]`** |
| Linux output | `Constant width` | Linux returns the message `almdisplay 4: Unable to connect to MultiVantage`. |
| Web interface | • Bold for **menu selections, tabs, buttons,** and **field names**<br>• Right arrow > to separate a sequence of menu selections | Select **Alarms and Notification,** the appropriate alarm, and then click **Clear**.<br>Select **Diagnostics** > **View System Logs**, then click **Watchdog Logs**. |
| Keys | Special font for keyboard keys and SAT screen clickable buttons | Press Tab.<br>Click Next Page. |

***(2 of 2)***

Other conventions used in this book:

- Physical dimensions are in English [Foot Pound Second (FPS)] units, followed by metric [Centimeter Gram Second) (CGS)] units in parentheses.
- Wire-gauge measurements are in AWG, followed by the diameter in millimeters in parentheses.
- Circuit-pack codes (such as TN790 or TN2182B) are shown with the minimum acceptable alphabetic suffix (for example, the "B" in the code TN2182B).

  Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every vintage of either the minimum suffix or a higher suffix code is necessarily acceptable.

# Useful terms

Table 3, Terminology summary, on page 22 summarizes some of the terms used in this book and relates them to former terminology.

**Table 3: Terminology summary**

| Present Terminology | Former Terminology |
|---|---|
| Communication Manager | MultiVantage<br>Avaya Call Processing |
| S8300 Media Server | ICC, Internal Call Controller |
| S8700 Media Server (or non-co-resident S8300) | ECC, External Call Controller |
| MGP, Media Gateway Processor | 860T Processor |
| Layer 2 Switching Processor | P330 Stack Processor<br>Cajun Stack Processor<br>i960 Processor |

# 1 Maintenance strategy

The maintenance subsystem is the part of a system's software that is responsible for initializing and maintaining the system. This subsystem continuously monitors the system's health and records detected errors. The maintenance subsystem also provides a user interface for on-demand testing.

This chapter provides a brief description of the maintenance strategy and presents background information about the system's overall functions. For detailed descriptions of components and subsystems, refer to related topics in the *Maintenance Alarms Reference (555-245-102)*. This chapter includes the following topics:



## Maintenance Objects

The system is partitioned into separate entities called maintenance objects (MOs). Each MO is monitored by the system and has its own maintenance strategy. A maintenance object can be:

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

Each MO is referred to by an upper-case, mnemonic-like name that serves as an abbreviation for the MO. For example, "CO-TRK" stands for "Central Office TRunK."

"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. These locations display as the `Port` field in the Alarm and Error logs and as output of various commands such as **test board**, **busy tdm-bus**, and so forth. The Maintenance Alarms Reference (555-245-102) includes the complete set of MOs and maintenance strategies.

Most MOs are individual circuit packs such as the:

- Direct Inward Dial Trunk circuit pack (DID-BD)
- DS1 Tie Trunk circuit pack (TIE-DS1)
- Expansion Interface (EI) circuit pack (EXP-INTF)

Some MOs represent hardware components that correside on a circuit pack. For example, the following circuit packs have the listed circuits residing on them:

- IP Server Interface circuit pack (IP-SVR) — Packet Interface (PKT-INT), IP Server Control (IPSV-CTL), Enhanced Tone Receiver (ETR-PT), TDM bus clock (TDM-CLK), Tone Generator (TONE-PT), and Tone-Clock (TONE-BD)
- **S8700 MC** Tone-Clock circuit pack (TONE-BD) (found in non-IPSI-connected port networks only) — TDM bus clock (TDM-CLK) and Tone Generator (TONE-PT).

Other MOs represent larger subsystems or sets of monitors, such as an expansion port network (EXP-PN) or a cabinet's environmental sensors (CABINET).

Finally, some MOs represent processes or combinations of processes and hardware, such as synchronization (SYNC) and duplicated port network connectivity (PNC-DUP). The previous abbreviations are *maintenance names* as recorded in the error and alarm logs. Individual copies of a given MO are further distinguished with an address that defines its physical location in the system. These addresses, along with repair instructions and a description of each MO appear alphabetically in *Maintenance Alarms Reference (555-245-102)*.

# Maintenance testing

Maintenance testing can reduce most troubles to the level of a field-replaceable component (usually a circuit pack). The affected circuits can be identified by:

- LEDs on the circuit packs
- Reports generated by the system software

## Background testing

The background maintenance tests in the system are divided into three groups:

- **Periodic** tests:
  - — Usually performed hourly by maintenance software
  - — Nondestructive (not service-affecting)
  - — Can be run during high-traffic periods without interfering with calls
- **Scheduled** tests:
  - — Usually performed daily
  - — More thorough than periodic testing
  - — Destructive (service-affecting)
  - — Run only during off-hours to avoid service disruptions

- **Fixed-interval** tests:
  - — Performed at regular time intervals and cannot be administered
  - — Run concurrently with periodic maintenance
  - — The MOs that run fixed-interval testing are listed below:

| Maintenance Object | Interval (min) |
|---|---|
| TDM-BUS | 10 |
| TONE-PT | 10 |

## Demand testing

Other kinds of maintenance testing are referred to as **Demand** tests.

- Include periodic tests plus other tests required only when trouble occurs.
- Can be run by the system when it detects a need or by maintenance personnel in trouble-clearing activities.
- Using the management terminal, maintenance personnel can “demand” the same tests that the system initiates in periodic or background testing.
- Some non-periodic demand tests are destructive (service-disrupting) tests, and are identified in boldface type.

---

**S8100 only**

# Co-Resident DEFINITY LAN Gateway maintenance

The Co-Resident DEFINITY LAN Gateway (DLG) provides connectivity for ASAI to ASAI adjuncts, including CentreVu-CT. Connectivity is provided between an S8100 Media Server and an ASAI adjunct using the interface on the TN2314 circuit pack and/or the C-LAN TN799 circuit pack.

The DLG functionality is co-resident on the S8100 Media Processor. This feature must be enabled in the license file. If it is enabled, the `Co-Res DEFINITY LAN Gateway?` field on the System-Parameters Customer-Options form is set to **y**.

The DLG CTI Link Status form is used to obtain a summary of the connections to the built-in DLG feature. See ADJ-IP/ASAI-IP (ASAI Adjunct IP Link) in *Maintenance Alarms Reference (555-245-102)*.

# Processor C-LAN maintenance

The Processor C-LAN provides TCP/IP connectivity to S8100 using the Ethernet interface on the TN2314 Processor Board. This is similar to the use of the C-LAN, except that the processor interface is specified. The Processor C-LAN connectivity is an option for specified applications, such as the DLG feature.

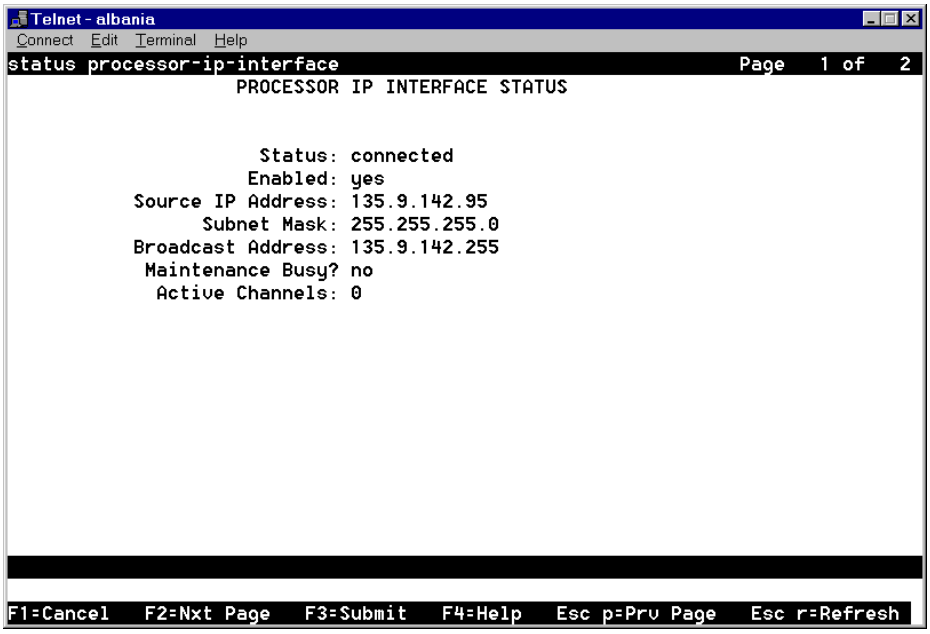
## Administration and maintenance

Before the LAN interface on the TN2314 processor card can be used, the `Processor Ethernet?` field must be enabled in the License File for this system. Display the System-Parameters Customer-Options form (**display system-parameters customer-options**), page 4, to check that this field is enabled (set to **y**).

The **status**, **busy**, and **release-from-busy** commands are available for the Processor Ethernet interface.

For more information on the **status** command see status processor-ip-interface in *Maintenance Commands Reference (555-245-101)* and Figure 1, Processor interface status, on page 26.

**Figure 1: Processor interface status**




# Media processor (DEFINITY ONE)

The MedPro board is the TN802B version of the MAPD circuit pack, when operating as a media processor. See MEDPROPT (TN802/TN2302 MED PRO DSP PORT) in *Maintenance Alarms Reference (555-245-102)*.

# Alarm and error reporting

During normal operations, software, hardware, or firmware may detect error conditions related to specific MOs. The system attempts to fix or circumvent these problems automatically. Errors are detected in two ways:

- For “in-line” errors, firmware on the component detects the occurrence of an error during ongoing operations.
- For other types of errors, a “periodic test” or a “scheduled test” started by the software detects the error.

  The technician can run periodic and scheduled tests on demand by using the maintenance commands described in *Maintenance Commands Reference (555-245-101)*, and the maintenance objects in *Maintenance Alarms Reference (555-245-102)*.

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 zero), there is a maintenance record for the MO. If a hardware component incurs too many errors, an alarm is raised.

## Alarm and error logs

The system keeps a record of every alarm that it detects. This record, the alarm log, and the error log can be displayed locally on the management terminal. An alarm is classified as major, minor, or warning, depending on its effect on system operation. Alarms are also classified as ON-BOARD or OFF-BOARD.

- MAJOR alarms identify failures that cause critical degradation of service and require immediate attention. Major alarms can occur on standby components without affecting service, since their active counterparts continue to function.
- MINOR alarms identify failures that cause some service degradation but do not render a crucial portion of the system inoperable. The condition requires attention, but typically a minor alarm affects only a few trunks or stations or a single feature.
- WARNING alarms identify failures that cause no significant degradation of service or failures of equipment external to the system. These are not reported to the Avaya alarm receiving system or the attendant console.
- ON-BOARD problems originate in circuitry on the alarmed circuit pack.
- OFF-BOARD problems originate in a process or component external to the circuit pack.

Multiple alarms against a given MO can change the level of a given alarm as it appears in the alarm log.

**Table 4: Multiple alarms against an MO**

| If... | And... | Then... |
|---|---|---|
| An active error causes a minor alarm | An active error causes a major alarm | The alarm log shows two major alarms. |
| The minor alarm is resolved first | | The error is marked as alarmed until the major alarm is resolved, and the alarm log shows two major alarms. |
| The major alarm is resolved first | | The error is marked as alarmed until the minor alarm is resolved, and the alarm log shows two minor alarms. |

An ON-BOARD alarm causes every alarm against that MO to report as ON-BOARD.

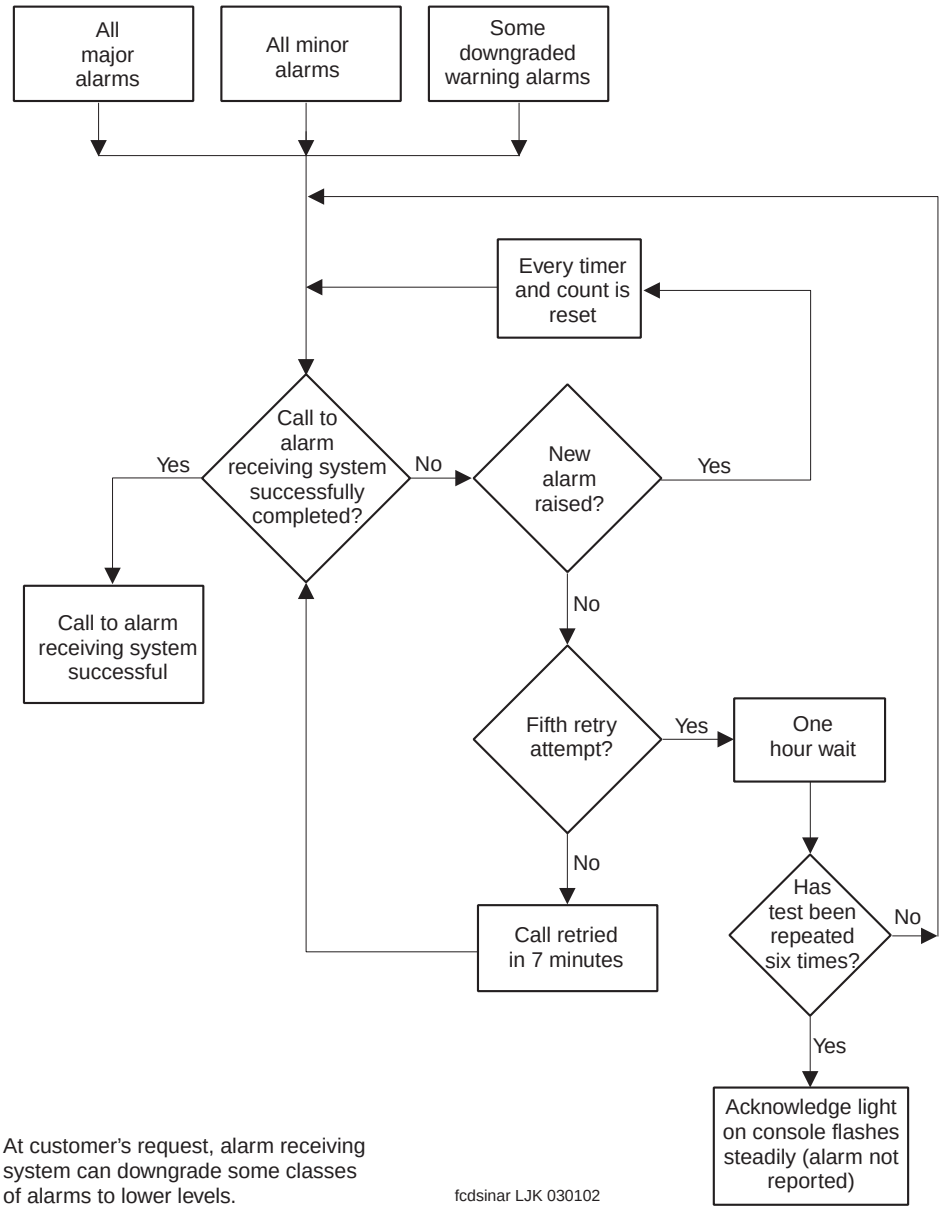
**NOTE:**
To determine the actual level and origin of each alarm when there are more than one against the same MO, see the Hardware Error Log Entries table for that MO.

The alarm log is restricted in size. If the log is full, a new entry overwrites the oldest resolved alarm. If there are no resolved alarms, the oldest error that is not alarmed is overwritten. If the full log consists of only active alarms, the new alarm is dropped and not recorded.

## Alarm reporting

Every major or minor alarm is reported to the Avaya alarm receiver system to generate a trouble report in the Avaya Services Ticketing System. Some warning alarms can be upgraded in conjunction with the Enhanced Remote Support (ERS) offer. These alarms are external to the product and the customer can choose these options for an additional charge (see Figure 2, Alarm reporting flowchart, on page 29).

**Figure 2: Alarm reporting flowchart**




# Power interruptions

System cabinets and their associated power supplies can be powered by 110/208 VAC, either directly or from an uninterruptible power supply (UPS) system. Alternatively, the cabinets and their power supplies may be powered by a -48 VDC battery power plant, which requires DC-to-DC conversion power units in the system.

If power is interrupted to a DC- or an AC-powered cabinet without optional backup batteries, the effect depends upon the decay time of the power distribution unit:

- If the interruption period is shorter than the decay time, there is no effect on service, though some -48V circuits may experience some impact.
- If the decay time is exceeded for an EPN, all service to that port network is dropped, and the EPN must be reset when power is restored.
- For **S8700 MC**, if the EPN contains a switch node carrier, all service to port networks connected to that switch node is dropped.

Single-carrier cabinets that are used as Expansion Port Networks (EPNs) have no battery backup. If power is interrupted for more than 0.25 seconds, all service is dropped and emergency transfer is invoked for the EPN.

In the above cases, the cabinet losing power is unable to log any alarms. However, in the case of an EPN going down while a server remains up, alarms associated with the EPN are reported by the system.

## Nominal power holdover

AC-powered multicarrier cabinets are equipped with an internal battery that is powered by its own charger and that provides a short-term holdover to protect the system against brief power interruptions. This feature, known as the nominal power holdover, is optional on cabinets supplied by a UPS and required on every other AC-powered cabinet. The battery is controlled in such a manner that it automatically provides power to the cabinet if the AC service fails. The duration of the holdover varies according to the cabinet's administration (see Table 5, Nominal power holdover, on page 30 for duration times).

**Table 5: Nominal power holdover**

| Cabinet administration | Control carrier holdover duration | Entire cabinet holdover duration |
|---|---|---|
| **a-carrier-only** | 10 minutes | 15 seconds |
| **all-carriers**[1] | 2 minutes | 2 minutes |

1 The cabinet should be administered to **all-carriers** only if the EPN maintenance board is a TN775D V2 or greater. However, since it is possible to administer the cabinet to **all-carriers** before there is connectivity to the EPN maintenance board, the administration may be incorrect. To verify whether your cabinet administration is correct, run **test maintenance *UU*** (where ***UU*** is the cabinet number). If it is incorrectly administered to **all-carriers**, a warning alarm will be issued and you should re-administer the cabinet to **a-carrier-only**.

## Power interruption effects

Power holdover is controlled by software to allow the system to sustain multiple brief power interruptions without exhausting the batteries before they have time to recharge. After power is restored, the batteries are recharged by a circuit that monitors current and time. If the batteries take more than 30 hours to recharge, a minor alarm is raised, indicating that the batteries must be replaced or the charger replaced.

The 397 Battery Charger Circuit immediately detects loss of AC power and raises a warning alarm against AC-POWER that is not reported to the Avaya alarm receiver system. Certain maintenance objects such as external DS1 timing report major alarms in this situation. When power is restored, the AC-POWER alarm is resolved.

## External alarm leads

Each cabinet provides two leads for one major and one minor alarm contact closure that can be connected to external equipment. These are located on the Maintenance circuit packs. If the switch is under warranty or a maintenance agreement, EXT-DEV alarms are generated by the equipment connected to these leads and reported to the Avaya alarm receiving system. These might be used to report failures of UPSs or battery reserves powering the switch. They are also commonly used to monitor adjuncts such as AUDIX.

# Protocols

This section describes the protocols handled by the system and the points where these protocols change. Figure 3, Intra-port and Inter-port data transmission states, on page 33 is a pictorial guide through intra-port and inter-port data transmission state changes. Figure 3, Intra-port and Inter-port data transmission states, on page 33 illustrates the flow of data from DTE equipment, like a terminal or host, through DCE equipment, like a modem or data module, into a communications port on the system. The data flow is shown by solid lines. Below these lines are the protocols used at particular points in the data stream.

Not shown in Figure 3, Intra-port and Inter-port data transmission states, on page 33 is the treatment of D-channels in ISDN-PRI and ISDN-BRI transmissions. PRI and BRI D channels transport information elements that contain call-signaling and caller information. These elements conform to ISDN level-3 protocol. In the case of BRI, the elements are created by the terminal or data module; for the PRI, the elements are created by the system, which inserts them into the D channel at the DS1 port.

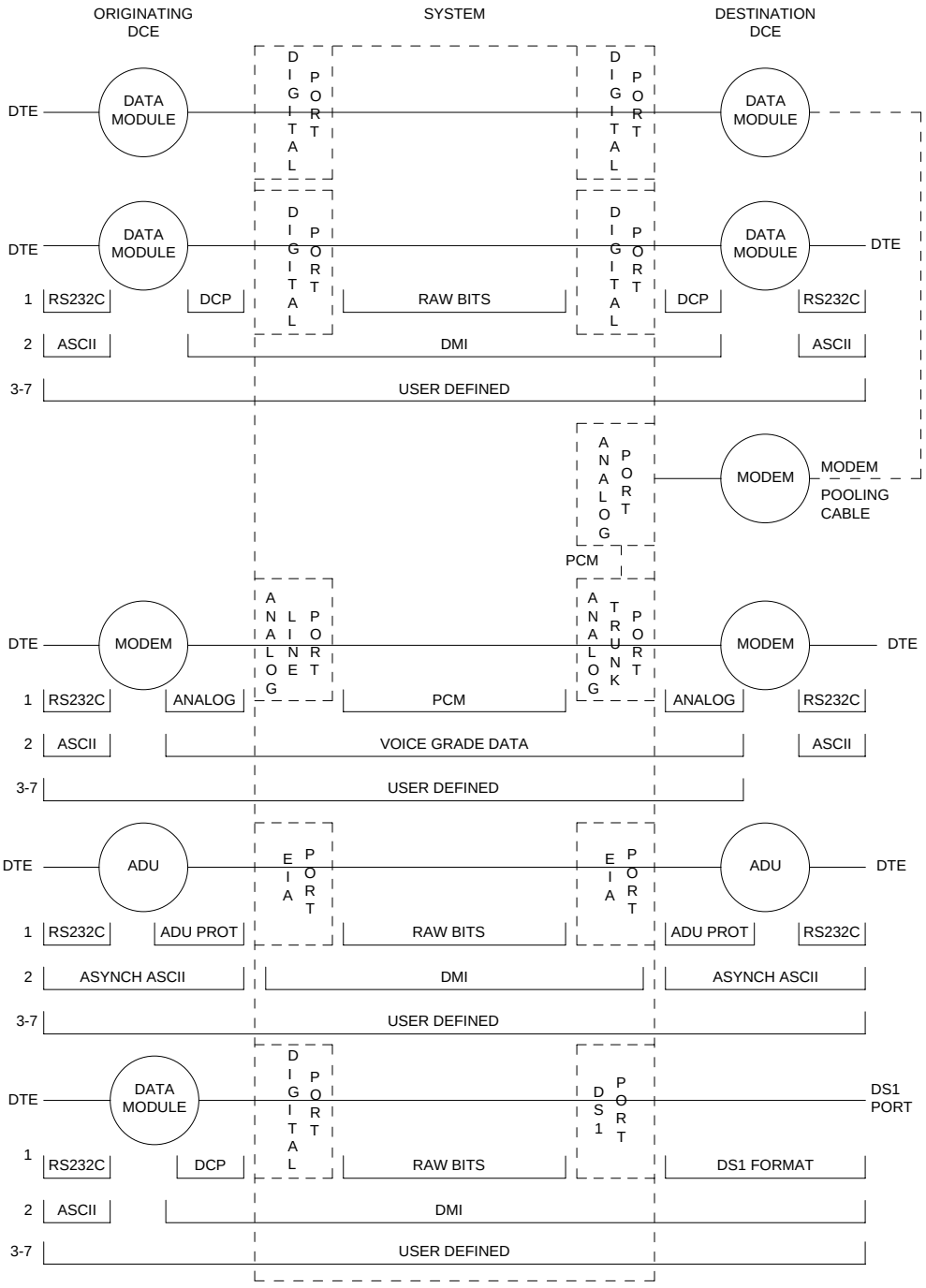
Therefore, for ISDN transmissions, BRI terminals and data modules, and DS1 ports insert, interpret, and strip both Layer-2 DCE information and Layer-3 elements. Also, the DS1 port passes Layer-3 elements to the system for processing. For more information about Layer 2 or 3, see OSI layers on page 32.

# OSI layers

The Open System Interconnect (OSI) model for data communications contains seven layers, each with a specific function. Communications to and through the system concern themselves only with Layers 1 and 2 of the model.

- Layer 1, or the *physical layer*, covers the physical interface between devices and the rules by which bits are passed. Among the physical layer protocols are RS-232, RS-449, X.21, DCP, DS1, and others.
- Layer 2, or the *data-link layer*, refers to code created and interpreted by the DCE. The originating equipment can send blocks of data with the necessary codes for synchronization, error control, or flow control. With these codes, the destination equipment checks the physical link's reliability, corrects any transmission errors, and maintains the link. When a transmission reaches the destination equipment, it strips any layer-2 information the originating equipment may have inserted. The destination equipment passes to the destination DTE equipment only the information sent by the originating DTE equipment. The originating DTE equipment can also add Layer-2 code to be analyzed by the destination DTE equipment. The DCE equipment treats this layer as data and passes it along to the destination DTE equipment as it would any other binary bits.
- Layers 3 to 7 (and the DTE-created layer 2) are embedded in the transmission stream and are meaningful only at the destination DTE equipment. Therefore, they are shown in Figure 3, Intra-port and Inter-port data transmission states, on page 33 as "user-defined," with no state changes until the transmission stream reaches its destination.

**Figure 3: Intra-port and Inter-port data transmission states**




## Usage

The following is a list of the protocols used when data is transmitted to and through the system. The list is organized by protocol layers. See Figure 3, Intra-port and Inter-port data transmission states, on page 33.

## Layer-1 protocols

Layer-1 protocols are used between the terminal or host DTE and the DCE, used between the DCE equipment and the system port, and used inside the system.

The following Layer-1 protocols are used between the DTE equipment and the DCE equipment. DCE equipment can be data modules, modems, or Data Service Units (DSUs). A DSU is a device that transmits digital data to a particular digital endpoint over the public network without processing the data through any intervening private network switches.

- *RS-232* — A common physical interface used to connect DTE to DCE**. This protocol is typically used for communicating up to 19.2 kbps.**
- *RS-449* — Designed to overcome the RS-232 distance and speed restrictions and lack of modem control
- *V.35* — A physical interface used to connect DTE to a DCE. This protocol is typically used for transmissions at 56 or 64 kbps.

The following protocols are used at Layer 1 to govern communication between the DCE equipment and the port. These protocols consist of codes inserted at the originating DCE and stripped at the port. The DS1 protocol can be inserted at the originating, outgoing trunk port and stripped at the destination port.

- *Digital Communications Protocol (DCP)* — A standard for a 3-channel link. This protocol sends *digitized* voice and digital data in frames at 160 kbps. The channel structure consists of two information (I) channels and one signaling (S) channel. Each I channel provides 64 kbps of voice and/or data communication, and the S channel provides 8 kbps of signaling communication between the system and DTE equipment. DCP is similar to ISDN BRI.
- *Basic Rate Interface (BRI)* — An ISDN standard for a 3-channel link, consisting of two 64-kbps bearer (B) channels and one 16-kbps signaling (D) channel.
- *Primary Rate Interface (PRI)* — An ISDN standard that sends digitized voice and digital data in T1 frames at 1.544-Mbps or, for countries outside the United States, in E1 frames at 2.048-Mbps. Layer 1 (physical), layer 2 (link), and layer 3 (network) ISDN-PRI protocols are defined in *DEFINITY Communications System and System 75/85 DSE/DMI/ISDN PRI Reference Manual*. At 1.544 Mbps, each frame consists of 24 64-kbps channels plus 8 kbps for framing. This represents 23 B channels plus 1 D channel. The maximum user rate is 64 kbps for voice and data. The maximum distances are based on T1 limitations. At 2.048 Mbps, each E1 frame consists of 32 64-kbps channels.
- *Analog* — A modulated voice-frequency carrier signal
- *ADU Proprietary* — A signal generated by an ADU. The signal is for communication over limited distances and can be understood only by a destination ADU or destination system port with a built-in ADU
- *Digital Signal Level 1 (DS1)* — A protocol defining the line coding, signaling, and framing used on a 24-channel line. Many types of trunk protocols (for example, PRI and 24th-channel signaling) use DS1 protocol at layer 1.
- *European Conference of Postal and Telecommunications rate 1 (CEPT1)* — A protocol defining the line coding, signaling, and framing used on a 32-channel line. Countries outside the United States use CEPT1 protocol.

Inside the system, data transmission appears in one of two forms:

- Raw digital data, where the physical layer protocols, like DCP, are stripped at the incoming port and reinserted at the outgoing port.
- Pulse Code Modulation (PCM)-encoded analog signals (analog transmission by a modem), the signal having been digitized by an analog-to-digital coder/decoder (CODEC) at the incoming port.

### Layer-2 protocols

Layer-2 protocols are given below:

- *8-bit character code* — Between the DTE and DCE equipment. Depending on the type of equipment used, the code can be any proprietary code set.
- *Digital multiplexed interface proprietary* — Between the originating and the destination DCE. Family of protocols for digital transmission.
- *Voice-grade data* — Between the originating and the destination DCE. For analog transmission.

## Protocol states

Table 6, Protocol states for data communication, on page 35 summarizes the protocols used at various points in the data transmission stream. See Figure 3, Intra-port and Inter-port data transmission states, on page 33.

**Table 6: Protocol states for data communication**

| Transmission type | Incoming DTE to DCE | OSI layer[1] | Protocols DTE to DCE | DCE to system port | Inside system |
|---|---|---|---|---|---|
| Analog | Modem | 1 | RS-232, RS-449, or V.35 | analog | PCM[2] |
| | | 2 | 8- or 10-bit code | Voice-grade data | Voice-grade data |
| | ADU | 1 | RS-232 | ADU proprietary | Raw bits |
| | | 2 | Asynchronous 8-bit code | Asynchronous 8-bit code | DMI[3] |
| Digital | Data Module | 1 | RS-232, RS-449, or V.35 | DCP or BRI | Raw bits |
| | | 2 | 8-bit code | DMI[3] | DMI[3] |
| | Digital Signal Level 1 (DS1) | 1 | Any | DS1 | PCM[2] or raw bits |
| | | 2 | 8-bit code | DMI[3] or voice-grade data | DMI[3] or voice-grade data |

1 OSI means Open Systems Interconnect
2 PCM means Pulse Code Modulated
3 DMI means Digital Multiplexed Interface

Both the physical-layer protocol and the Digital Multiplexed Interface (DMI) mode used in the connection are dependent upon the type of 8-bit code used at layer 2 between the DTE and DCE equipment, as listed in Table 7, Physical-layer protocol versus character code, on page 36 and Table 8, Digital Multiplexed Interface (DMI) mode versus character code, on page 36.

**Table 7: Physical-layer protocol versus character code**

| Protocol | Code |
|---|---|
| RS-232 | Asynchronous 8-bit ASCII, and synchronous |
| RS-449 | Asynchronous 8-bit ASCII, and synchronous |
| V.35 | Synchronous |

**Table 8: Digital Multiplexed Interface (DMI) mode versus character code**

| DMI Mode | Code |
|---|---|
| 0 | Synchronous (64 kbps) |
| 1 | Synchronous (56 kbps) |
| 2 | Asynchronous 8-bit ASCII (up to 19.2 kbps), and synchronous |
| 3 | Asynchronous 8-bit ASCII, and private proprietary |

## Connectivity rules

Figure 3, Intra-port and Inter-port data transmission states, on page 33 implies the following connectivity rules:

- Only the DS1 port and the analog trunk port are trunking facilities (every other port is a line port). For communication over these facilities, the destination DCE equipment can be a hemisphere away from the system, and the signal can traverse any number of intervening switching systems before reaching the destination equipment.
- Data originating at any type of digital device, whether DCP or BRI, can exit the system at any type of digital port — BRI, digital-line, PRI, DS1, and others; as long as the call destination is equipped with a data module using the same DMI mode used at the call origin. This is because once the data enters the system through a digital port, its representation is uniform (raw bits at layer 1, and DMI at level 2), regardless of where it originated.
- Although data entering the system through an EIA port has not been processed through a data module, the port itself has a built-in data module. Inside the system, port data is identical to digital line data. Data entering the system at a DCP line port can exit at an EIA port. Conversely, data entering the system at an EIA port can exit at any DCP line port. The destination data module must be set for Mode-2 DMI communication.
- Voice-grade data can be carried over a DS1 facility as long as the destination equipment is a modem compatible with the originating modem.
- If a mismatch exists between the types of signals used by the endpoints in a connection (for example, the equipment at one end is an analog modem, and the equipment at the other end is a digital data module), a modem-pool member must be inserted in the circuit. When the endpoints are on different switches, it is recommended that the modem-pool member be put on the

origination or destination system. A modem-pool member is always inserted automatically for calls to off-premises sites via analog or voice-grade trunking. For internal calls, however, the systems are capable of automatically inserting a modem-pool member.

- Data cannot be carried over analog facilities unless inside the system it is represented as a PCM-encoded analog signal. To do this for data originating at a digital terminal, the signal enters the system at a digital port and exits the system at a digital port. The signal then reenters the system through a modem-pool connection (data-module to modem to analog-port) and exits the system again at an analog port.
- Although DS1 is commonly called a trunk speed, here it names the protocol used at layer 1 for digital trunks. Some trunks use different signaling methods but use DS1 protocol at layer 1 (for example, PRI and 24th-channel signaling trunks).

# Signaling

This section describes disconnect supervision and transmission characteristics.

## Disconnect supervision

Disconnect supervision means the CO has the ability to release a trunk when the party at the CO disconnects and the system is able to recognize the release signal. In general, a CO in the United States provides disconnect supervision for incoming calls but not for outgoing calls. Many other countries do not provide disconnect supervision for either incoming or outgoing calls.

The system must provide the assurance that at least one party on the call can control dropping the call. This avoids locking up circuits on a call where no party is able to send a disconnect signal to the system. Internal operations must check to ensure that one party can provide disconnect supervision. An incoming trunk that does not provide disconnect supervision is not allowed to terminate to an outgoing trunk that does not provide disconnect supervision.

In a DCS environment an incoming trunk without disconnect supervision can terminate to an outgoing DCS trunk connecting two nodes. The incoming trunk is restricted from being transferred to a party without disconnect supervision on the terminating node. This is because through messaging the terminating node knows that the originating node cannot provide disconnect supervision. This messaging is not possible with non-DCS tie trunks, and the direct call is denied.

Administration is provided for each trunk group to indicate whether it provides disconnect supervision for incoming calls and for outgoing calls.

### Transfer on ringing

A station or attendant may conference in a ringing station or transfer a party to a ringing station. When a station conferences in a ringing station and then drops the call, the ringing station is treated like a party without disconnect supervision. However, when a station transfers a party to a ringing station, the ringing station party is treated like a party with disconnect supervision. Two timers (Attendant Return Call Timer and Wait Answer Supervision Timer) are provided to ensure the call is not locked to a ringing station.

### Conference, Transfer, and Call-Forwarding Denial

If a station or attendant attempts to connect parties without disconnect supervision together, the outcomes listed in Table 9, Attempted connection without disconnect supervision, on page 38 are possible.

**Table 9: Attempted connection without disconnect supervision**

| Attempted activity | Possible outcome |
|---|---|
| Digital station or local attendant transfer | If a digital station attempts to transfer the two parties together, the call-appearance lamp flutters, indicating a denial. If transferring over a DCS trunk, the denial may drop the call since the transfer is allowed, and the other system is queried for disconnect supervision. |
| Analog station transfer | If an analog station attempts to transfer two parties together by going on-hook, the analog station is no longer on the call and the transfer cannot be denied. |
| Centralized Attendant Service (CAS) transfer | If a CAS attempts to transfer two parties together by pressing the release key, the release link trunk is released and the branch attempts a transfer by hanging up. |
| Station Conference/Dropout | If a station conferences every party, the conference is allowed since the station has disconnect supervision. When the station is dropped from the call, the call is dropped since the other parties do not have disconnect supervision. |
| Station Call Forwarding | If a station is call forwarded off-premise to a trunk without disconnect supervision, the calling party without disconnect supervision is routed to the attendant. |

## Transmission characteristics

The system's transmission characteristics comply with the American National Standards Institute/Electronic Industries Association (ANSI/EIA) standard RS-464A (SP-1378A).

## Frequency response

Table 10, Analog-to-analog frequency response, on page 39 lists the analog-to-analog frequency response for station-to-station or station-to-CO trunk, relative to loss at 1 kHz for the United States.

**Table 10: Analog-to-analog frequency response**

| Frequency (Hz) | Maximum loss (dB) | Minimum loss (dB) |
|---|---|---|
| 60 | – | 20 |
| 200 | 5 | 0 |
| 300 to 3000 | 1 | -0.5 |
| 3200 | 1.5 | -0.5 |
| 3400 | 3 | 0 |

Table 11, Analog-to-digital frequency response, on page 39 lists the analog-to-digital frequency response of the system for station or CO-trunk-to-digital interface (DS0), relative to loss at 1 kHz for the United States.

**Table 11: Analog-to-digital frequency response**

| Frequency (Hz) | Maximum loss (dB) | Minimum loss (dB) |
|---|---|---|
| 60 | – | 20 |
| 200 | 3 | 0 |
| 300 to 3000 | 0.5 | -0.25 |
| 3200 | 0.75 | -0.25 |
| 3400 | 1.5 | 0 |

## Insertion loss

Table 12, Insertion loss (United States), on page 40 lists the insertion loss in the system for port-to-port, analog, or digital connections in the United States.

**Table 12: Insertion loss (United States)**

| Typical connections | Nominal loss (dB) at 1 kHz |
|---|---|
| On-premises to on-premises station | 6 |
| On-premises to off-premises station | 3 |
| Off-premises to off-premises station | 0 |
| On-premises station to 4-wire trunk | 3 |
| Off-premises station to 4-wire trunk | 2 |
| Station-to-trunk | 0 |
| Trunk-to-trunk | 0 |

Table 13, Overload and crosstalk, on page 40 shows the overload and cross-talk.

**Table 13: Overload and crosstalk**

| | |
|---|---|
| Overload level | +3 dBm0 |
| Crosstalk loss | >70 dB |

## Intermodulation distortion

Table 14, Intermodulation distortion, on page 40 lists the intermodulation distortion in the system for analog-to-analog and analog-to-digital, up to 9.6 kbps data.

**Table 14: Intermodulation distortion**

| Four-tone method | Distortion |
|---|---|
| Second-order tone products | >46 dB |
| Third-order tone products | >56 dB |

## Quantization distortion loss

Table 15, Quantization distortion loss (analog port-to-analog port), on page 41 lists the quantization distortion loss in the system for analog port to analog port.

**Table 15: Quantization distortion loss (analog port-to-analog port)**

| Signal level | Distortion loss |
|---|---|
| 0 to -30 dBm0 | >33 dB |
| -40 dBm0 | >27 dB |
| -45 dBm0 | >22 dB |

Table 16, Quantization distortion loss, on page 41 lists the quantization distortion loss in the system for analog port-to-digital port and digital port-to-analog port.

**Table 16: Quantization distortion loss[1]**

| Signal level | Distortion loss |
|---|---|
| 0 to -30 dBm0 | >35 dB |
| -40 dBm0 | >29 dB |
| -45 dBm0 | >25 dB |

1 Terminating Impedance: 600 Ohms nominal
Trunk balance impedance (selectable): 600 Ohms nominal or complex Z [350 Ohms + (1 k Ohms in parallel with 0.215uF)]

## Impulse noise

On 95% or more of all connections, the impulse noise is 0 count (hits) in 5 minutes at +55 dBrnC (decibels above reference noise with C-filter) during the busy hour.

## ERL and SFRL talking state

Echo-Return Loss (ERL) and Single-Frequency Return Loss (SFRL) performance are usually dominated by termination and/or loop input impedances. The system provides an acceptable level of echo performance if the ERL and SFRL are met, as follows:

**Table 17: ERL and SFRL performances by connection type**

| Type of connection | ERL and SFRL performance |
|---|---|
| Station-to-station | ERL should meet or exceed 18 dB<br>SFRL should meet or exceed 12 dB |
| Station to 4-wire trunk connection | ERL should meet or exceed 24 dB<br>SFRL should meet or exceed 14 dB |
| Station to 2-wire trunk connection | ERL should meet or exceed 18 dB<br>SFRL should meet or exceed 12 dB |
| 4-wire to 4-wire trunk connection | ERL should meet or exceed 27 dB<br>SFRL should meet or exceed 20 dB |

### Peak noise level

Table 18, Peak noise level, on page 42 shows the peak noise level.

**Table 18: Peak noise level**

| Type of connection | Peak noise level (dBrnC)[1] |
|---|---|
| Analog to analog | 20 |
| Analog to digital | 19 |
| Digital to analog | 13 |

1 Decibels above reference noise with C-filter

### Echo path delay

- Analog port to analog port — ≤ 3 ms
- Digital interface port to digital interface port — ≤ 2 ms

# Service codes

Service codes (for the United States only) are issued by the Federal Communications Commission (FCC) to equipment manufacturers and registrants. These codes denote the:

- Type of registered terminal equipment
- Protective characteristics of the premises wiring of the terminal equipment ports

Private-line service codes are as follows:

- 7.0Y — Totally protected private communications (microwave) systems
- 7.0Z — Partially protected private communications (microwave) systems
- 8.0X — Port for ancillary equipment
- 9.0F — Fully protected terminal equipment
- 9.0P — Partially protected terminal equipment
- 9.0N — Unprotected terminal equipment
- 9.0Y — Totally protected terminal equipment

The product line service code is 9.0F, indicating it is terminal equipment with fully protected premises wire at the private line ports.

# Facility Interface Codes

A Facility Interface Code (FIC) is a 5-character code (United States only) that provides the technical information needed to order a specific port circuit pack for analog private lines, digital lines, MTS lines, and WATS lines.

Table 19, Analog private line and trunk port circuit packs, on page 43 through Table 21, MTS and WATS port circuit packs, on page 43 list the FICs. Included are service order codes, Ringer Equivalency Numbers (RENs), and types of network jacks that connect a line to a rear panel connector on a carrier.

**Table 19: Analog private line and trunk port circuit packs**

| Circuit Pack | FIC | Service order code | Network jack |
|---|---|---|---|
| TN742 and TN747B Off-Premises Station Port<br>and<br>TN746B Off- or On-Premises Station Port | 0L13C | 9.0F | RJ21X |
| TN760/B/C/D Tie Trunk | TL31M | 9.0F | RJ2GX |

**Table 20: Digital trunk port circuit packs**

| Circuit Pack | FIC | Service Order Code | Network Jack |
|---|---|---|---|
| TN1654 and TN574 DS1 Converter; TN722B DS1 Tie Trunk; and TN767 and TN464 DS1 Interface | 04DU9B, C | 6.0P | RJ48C and RJ48M |

**Table 21: MTS and WATS port circuit packs**

| Circuit Pack | FIC | Ringer Equivalency Number (REN) | Network Jack |
|---|---|---|---|
| TN742 and TN746B Analog Line | 02LS2 | None | RJ21 and RJ11C |
| TN747B Central Office Trunk | 02GS2 | 1.0A | RJ21X |
| TN753 DID Trunk | 02RV2-T | 0,0B | RJ21X |
| TN790 Processor | 02LS2 | 1.0A | RJ21X |
| TN1648 System Access and Maintenance | 02LS2 | 0.5A | RJ21X |

# Multimedia Interface (MMI)

The Multimedia Interface handles the following protocols:

- International Telecommunications Union (ITU) H.221 — Includes H.230, H.242, H.231, and H.243 protocols
- American National Standards Institute (ANSI) H.221 — Includes H.230, H.242, H.231, and H.243 protocols
- BONDING (Bandwidth On-Demand Interoperability Group) Mode 1
- ESM HLP HDLC Rate Adaptation

The Vistium Personal Conferencing System is supported either through the 8510T BRI terminal or directly through the Vistium TMBRI PC board.

Using the World Class Core (WCC) BRI interface, most desktop multimedia applications are supported through a personal computer's BRI interface.

# S8300 and G700 maintenance strategy

The maintenance strategy is intended to provide easy fault isolation procedures and to limit problems to field-replaceable components. The maintenance strategy is driven by the desire to move the G700 toward a data networking paradigm. This leads to a dual strategy in which some of the G700's subsystems are maintained and controlled by a Media Server running Avaya Communication Manager, while others are covered by maintenance software residing on the G700. The latter subsystems are not monitored directly by a Media Server.

Table 22, Avaya Media Servers and Gateways maintenance arenas, on page 44 shows the three main maintenance arenas associated with the S8300 Media Server with G700 Media Gateways:

**Table 22: Avaya Media Servers and Gateways maintenance arenas**

| Arena | Detail |
|---|---|
| Web Interface | Web-based access to the S8300/S8700 Media Server. Users can perform administration, maintenance, and status functions through the Web interface. |
| Communication Manager System Access Terminal (SAT) commands | Very similar to standard Communication Manager SAT commands that readers are familiar with from other Avaya products |
| G700 CLI commands — see Chapter 4, "G700 MGP CLI Commands" in *Maintenance Commands Reference (555-245-101).* | Unique to the G700 Media Gateway platform. Used for administration, maintenance, and status functions on the G700. Users can also access the Layer 2 Switching Processor CLI for Layer 2 Switching Processor-related CLI commands) |

# Media Module maintenance

Media Module maintenance is controlled by 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 G700 (hot swap).

## Hot swap

The following Avaya Media Modules are hot-swappable:

- DCP Media Module (MM712)
- Analog Trunk/Telephone Port Media Module (MM711)
- T1/E1 Media Module (MM710)
- VoIP Media Module (MM760)
- BRI Media Module (MM720)

For procedures on adding, removing, or replacing Media Modules, refer to Replacing Media Modules on page 299.

**CAUTION:**
The S8300 Media Server is NOT hot swappable and can reset the entire G700 upon insertion or removal, as well as resetting each G700 that is currently registered with it. When removing the S8300, initiate a shutdown process by first depressing the button (for 2 seconds) located next to the fourth GREEN “Ok-to-Remove” LED (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. See Replacing the S8300 Media Server or hard drive on page 290.

**NOTE:**
This server can be a primary server for a network of IP endpoints and G700 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:**
If you remove the S8300 before the disk is shut down, you may corrupt important data. See Replacing the S8300 Media Server or hard drive on page 290.

**CAUTION:**
The Avaya Expansion Modules and Cascade Modules — are NOT hot-swappable. They are service-disrupting and can reset the entire G700 upon insertion or removal. Power down the system, including shutting down the S8300 hard drive, if present, prior to any insertion or removal of Avaya Expansion and Cascade modules.

## Access to the G700 Media Gateway and S8300 Media Server

You can access the Avaya Media Servers in several ways:

- Web server access to the Avaya Media Server IP address (Accesses Web page with Online Help)
- Telnet from customer LAN to the:
  - Server's IP address
  - Media Gateway Processor IP address
  - Layer-2 Switching Processor IP address
- Through the Layer 2 Switching Processor IP address (Accesses the Device Manager)
- Telnet to the server's IP address to port 5023 to get Communication Manager access
- Through Avaya Site Administration
- Remote access through a PPP link
- Through a serial cable

**NOTE:**
For detailed access and login procedures, refer to Chapter 2, "Access and login procedures".

## S8300 Media Server Web interface

The browser-based Web administration interface is used to administer the S8300 Media Server with the G700 Media Gateway on the corporate local area network (LAN). This administration interface via the Web is an efficient way to configure the S8300 Media Server with G700 Media Gateway. In addition to initial administration, it allows you to check server status, perform software and firmware upgrades, and 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 G700 Media Gateway. For more detailed information on access and login procedures, see Connection overview on page 59.

## G700 Media Gateway Processor CLI

The G700 Media Gateway Processor Command Line Interface (MGP CLI) provides access to configurable and read-only data of all G700 subsystems as well as running tests and displaying results. As a minimum, the MGP CLI supports all functionality the Device Manager provides. It provides access to the status, parameters, and/or test of Media Modules, IP Entity Configuration, TFTP Servers, and DSP/VoIP resources. Chapter 4, "G700 MGP CLI Commands" in *Maintenance Commands Reference (555-245-101)* provides a detailed description of each MGP CLI command.

## Layer 2 Switching Processor CLI

The Layer 2 Switching Processor CLI manages the layer 2 switching of the entire “stack.” The “stack” contains up to ten components (Layer 2 switches and/or additional G700 Media Gateways), assembled into a larger logical switch that is presented as a single network element to system management.

For more information about the L2 Processor CLI refer to *Avaya P330 Manager User Guide*.

# G700 server-controlled maintenance

## DEFINITY equivalent elements

Many of the Avaya Media Modules and G700 subsystems are based on existing DEFINITY circuit packs or systems as listed in Table 23, DEFINITY equivalent elements, on page 47. DEFINITY server-experienced users will find that components function and are maintained equivalently to their DEFINITY counterparts.

**NOTE:**
This information is included for environments where the G700 Media Gateway with an Avaya Media Server is integrated into larger architectures running Avaya Communication Manager.

**Table 23: DEFINITY equivalent elements**

| G700 component | DEFINITY equivalent |
|---|---|
| T1/E1 Media Module | Partially the TN464GP DS1 |
| Analog Line/Trunk Media Module | TN797 Combination Port Board |
| DCP Media Module | TN2224 2-Wire Digital Line Board |
| BRI Trunk Media Module | TN2185 BRI Board |
| Voice Announcement | TN2501 Announcement Board |
| S8300 | S8700 or other DEFINITY ECS |
| Messaging | CWY1 Board (DEFINITY One) |
| Tone Generator | TN2182 Tone Generator/Clock |
| Tone Detectors (DSP Emulated) | TN2182 ETR Ports |
| VoIP DSPs | TN2302AP DSP Farm (TN3201 AP DSP Farm) |

The actual implementation of circuits does differ markedly from their DEFINITY counterparts which, along with the G700, changes how many operations are conducted. The intent of G700 development is to move towards the data networking paradigm and to lessen the G700's and its components' dependency on Media Servers. Presumably, administration would eventually come from system management rather than

a Media Server. Another goal is to create “smarter” Media Modules which, when combined with enhancements of the G700’s maintenance software, allow all Media Module testing to occur on the G700 platform. Test results are sent to system management.

## Capacity constraints and feature limitations

Although Media Modules and other G700 components have functionality similar to DEFINITY server components, there are some differences. For example, the DCP MM supports 8 ports, while the TN2224 supports 24 ports. In addition, the hardware associated with some of the components differs significantly from the DEFINITY server version.

These differences, as well as the fact that the G700 has control over the TDM bus, the tone/clock generator, and the tone detectors means that a Media Server does not have any knowledge of those components. In addition, any facet of port maintenance that deals with packet bus maintenance or system synchronization will not be provided by the G700.

See Table 24, Media module tests, on page 49 for a complete list of the allowable and invalid tests for the G700 Media Modules. As shown in this table, the board and port tests are based on existing tests that run on the equivalent DEFINITY server port boards and the associated ports. Some tests abort with abort code 1412 to indicate that these tests cannot be run on a Media Module Maintenance Object by maintenance software on Avaya Media Servers.

**NOTE:**
No alarms are generated for failures detected by tests that are specified to abort for Media Modules.

**Table 24: Media module tests**

| Media Module | Maintenance Object | Test | Executed for Media Module |
|---|---|---|---|
| Analog Media Module (DEFINITY server TN797) | Board (ANA-MM) (DEF TR-LN-BD) | NPE Audit Test (#50) | Abort |
| | | Ringing Application Test (#51) | Yes |
| | | Control Channel Looparound Test (#52) | Yes |
| | | SAKI Sanity Test (#53) | Yes |
| | Analog Line (ANL-LN-PT) | NPE Crosstalk Test (#6) | Abort |
| | | Conference Test (#7) | Abort |
| | | Battery Feed Test (#35) | Yes |
| | | Station Status and Translation Audits and Updates Test (#36) | Yes |
| | | Station Present Test (#48) | Yes |
| | | Looparound Test (#161) | Abort |
| | Analog Co Trunk (CO-TRK) | Dial Tone Test (#0) | Abort |
| | | CO Demand Diagnostic Test (#3) | Yes |
| | | NPE Crosstalk Test (#6) | Abort |
| | | Looparound and Conference Test (#33) | Abort |
| | | Audit Update Test (#36) | Yes |
| | | Transmission Test - ATMS (#844-848) | Abort |
| | Analog DID Trunk (DID-TRK) | NPE Crosstalk Test (#6) | Abort |
| | | Looparound and Conference Test (#33) | Abort |
| | | Port Diagnostic Test (#35) | Yes |
| | | Port Audit Update Test (#36) | Yes |
| | DIOD Trunk (DIOD-TRK) | Dial Tone Test (#0) | Abort |
| | | NPE Crosstalk Test (#6) | Abort |
| | | Looparound and Conference Test (#33) | Abort |
| | | Audit Update Test (#36) | Yes |
| | Alarm Port (ALARM-PT) | Battery Feed Test (#35) | Yes |
| | | Station Status and Translation Audits and Updates Test (#36) | Yes |

*(1 of 6)*

**Table 24: Media module tests**

| Media Module | Maintenance Object | Test | Executed for Media Module |
|---|---|---|---|
| BRI Trunk Media Module (MM720) (DEF TN2185) | Board (MG-BRI) (DEF TBRI-BD) | NPE/NCE Audit Test (#50) | Abort |
| | | Control Channel Looparound Test (#52) | Yes |
| | | LAN Receive Parity Error Counter Test (#595) | Yes |
| | | SAKI Sanity Test (#53) | Yes |
| | ISDN Trunk Side BRI Port (TBRI-PT) | Clear Errors Counters Test (#270) | Yes |
| | | NPE Crosstalk Test (#617) | Abort |
| | | BRI Local LAN Port Looparound Test (#618) | Abort |
| | | BRI TDM Port Looparound Test (#619) | Abort |
| | | CRC Error Counter Test (#623) | Yes |
| | | Receive FIFO Overflow Test (#625) | Yes |
| | | L1 State Query Test (#1242) | Abort |
| | | Layer 3 Query Test (#1243) | Yes |
| | | Slip Query Test (#1244) | Yes |
| | ISDN Trunk Side BRI Signaling (TBRI-TRK) | Service State Audit Test (#256) | Yes |
| | | Call State Audit Test (#257) | Yes |
| | | ISDN Test Call Test (#258) | Abort |
| | | Signaling Link State Check Test (#1251) | Yes |

***(2 of 6)***

**Table 24: Media module tests**

| Media Module | Maintenance Object | Test | Executed for Media Module |
|---|---|---|---|
| BRI Trunk Media Module (DEFINITY TN2185) | Board (BRI-MM) (DEF TBRI-BD) | NPE/NCE Audit Test (#50) | Abort |
| | | Control Channel Looparound Test (#52) | Abort |
| | | LAN Receive Parity Error Counter Test (#595) | Yes |
| | | SAKI Sanity Test (#53) | Yes |
| | ISDN Trunk Side BRI Port (TBRI-PT) | Clear Error Counters Test (#270) | Yes |
| | | NPE Crosstalk Test (#617) | Abort |
| | | BRI Local LAN Port Loop Around Test (#618) | Abort |
| | | BRI TDM Port Loop Around Test (#619) | Abort |
| | | CRC Error Counter Test (#623) | Yes |
| | | Receive FIFO Overflow Test (#625) | Yes |
| | | L1 State Query Test (#1242) | Abort |
| | | Layer 3 Query Test (#1243) | Yes |
| | | Slip Query Test (#1244) | Yes |
| | ISDN Trunk Side Signaling (TBRI-TRK) | Service State Audit Test (#256) | Yes |
| | | Call State Audit Test (#257) | Yes |
| | | ISDN Test Call Test (#258) | Abort |
| | | Signaling Link State Check Test (#1251) | Yes |

***(3 of 6)***

**Table 24: Media module tests**

| Media Module | Maintenance Object | Test | Executed for Media Module |
|---|---|---|---|
| DCP Media Module (DEFINITY server TN2224) | Board (MG-DCP) (DEF DIG-BD) | NPE Audit Test (#50) | Abort |
| | | Control Channel Loop Test (#52) | Yes |
| | | SAKI Sanity Test (#53) | Yes |
| | Digital Line (DIG-LINE) | Digital Line NPE Crosstalk Test (#9) | Abort |
| | | Digital Line Electronic Power Feed Test (#11) | Yes |
| | | Voice and Control Channel Local Looparound Test (#13) | Abort |
| | | DIG-LINE Station Lamp Updates (#16) | Yes |
| | | Station Audits Test (#17) | Yes |
| | | Digital Terminal Remote Loop Around Test (#1201) | Abort |
| T1/E1 Media Module (DEF TN464F) | Board (MG-DS1) (DEF UDS1-BD) | NPE Correction Audit Test (#50) | Abort |
| | | Control Channel Loop Test (#52) | Yes |
| | | Loss of Signal Alarm Inquiry Test (#138) | Yes |
| | | Blue Alarm Inquiry Test (#139) | Yes |
| | | Red Alarm Inquiry Test (#140) | Yes |
| | | Yellow Alarm Inquiry Test (#141) | Yes |
| | | Major Alarm Inquiry Test (#142) | Yes |
| | | Minor Alarm Inquiry Test (#143) | Yes |
| | | Slip Alarm Inquiry Test (#144) | Yes |
| | | Misframe Alarm Inquiry Test (#145) | Yes |
| | | Translation Update Test (#146) | Yes |
| | | ICSU Status LEDs Test (#1227) | No |
| | | Echo Cancellation Test (#1420) | Yes |
| | | SAKI Sanity Test (#53) | Yes |
| | | Internal Loop Around Test (#135) | Abort |

***(4 of 6)***

**Table 24: Media module tests**

| Media Module | Maintenance Object | Test | Executed for Media Module |
|---|---|---|---|
| | DS1 CO Trunk (CO-DS1) | NPE Crosstalk Test (#6) | Abort |
| | | Conference Test (#7) | Abort |
| | | Port Audit and Update Test (#36) | Yes |
| | | DS1 CO Trunk Seizure Test (#314) | Abort |
| | DS1 DID Trunk (DID-DS1) | NPE Crosstalk Test (#6) | Abort |
| | | Conference Test (#7) | Abort |
| | | Port Audit and Update Test (#36) | Yes |
| | DS1 Tie Trunk (TIE-DS1) | NPE Crosstalk Test (#6) | Abort |
| | | Conference Test (#7) | Abort |
| | | Port Audit and Update Test (#36) | Yes |
| | | DS1 Tie Trunk Seizure test (#136) | Yes |
| | DS1 ISDN Trunk (ISDN-TRK) | NPE Crosstalk Test (#6) | Abort |
| | | Conference Test (#7) | Abort |
| | | Port Audit and Update Test (#36) | Yes |
| | | Signaling Line State Check Test (#255) | Yes |
| | | Service State Audit Test (#256) | Yes |
| | | Call State Audit Test (#257) | Yes |
| | | ISDN Test Call Test (#258) | Abort |
| | ISDN-PRI Signaling Link Port (ISDN-LNK) | NPE Crosstalk Test (#6) | Abort |
| | | PRI Port Test (#643) | Yes |
| | ISDN-PRI Signaling Group (ISDN-SGRP) | Primary Signaling Link Hardware Check (#636) | Yes |
| | | Secondary Signaling Link Hardware Check (#639) | Yes |
| | | Layer 2 Status Test (#647) | Yes |
| | Wideband Access Endpoint Port (WAE-PORT) | Remote Layer 3 Query Test (#637) | Yes |
| | | Looparound and Conference Test (#33) | Abort |
| | | Port Audit and Update Test (#36) | Yes |

***(5 of 6)***

**Table 24: Media module tests**

| Media Module | Maintenance Object | Test | Executed for Media Module |
|---|---|---|---|
| Voice Announcements (DEFINITY server TN2501AP) | Board (MG-ANN) | Control Channel Loop Test (#52) | Yes |
| | | Invalid LAPD Frame Error Counter Test (#597) | NA |
| | | PPE/LANBIC Receive Parity error Counter Test (#595) | NA |
| | | Receive FIFO Overflow Error Counter Test (#596) | NA |
| | | Packet Interface test (#598) | NA |
| | | Congestion Query Test (#600) | NA |
| | | Link Status test (#601) | NA |
| | Announcement Ports (VAL-PT) | Synchronous Loop Around Test (#1275) | Yes |
| | | Port Error Counter Test (#1280) | Yes |
| | | TDM Loop Around Test (#1285) | Abort |
| | Ethernet Port (ETH-PT) | Link Integrity Inquiry (#1282) | NA |
| | | Ethernet Local Loop Around Test (#1278) | NA |
| | | TCP/IP Ping Test (#1281) | NA |
| | | Session Status Test (#1286) | NA |
| Messaging | Board (MG-MSG) (DEF 1 PR-SSP) | Control Channel Loop Test (#52) | Yes |
| | | Board Diagnostic Test (#1350) | Yes |
| | | Time Slot Manager Test (#1358) | Yes |
| | Ports (PR-ADX) | Port Looparound Test (#1351) | Abort |

***(6 of 6)***

# Testing

G700 subsystems that are under the control of S8300/S8700 Media Servers running Communication Manager have a limited degree of functionality. Due to the different system architectures, the full range of tests is not available.

## Tests not executed on the G700

Table 25, Tests not executed on the G700 platform, on page 55 indicates why some tests are not executed on the G700.

**Table 25: Tests not executed on the G700 platform**

| Test | Notes |
|---|---|
| NPE_AUDIT | This test is really an audit that sends network update messages to various ports on a board. Since the Media server does not handle network connections for the MG, this test is not run. |
| DS1_DTONE_TS | DS1 CO trunk dial tone seizure test |
| NEON_TEST | This is run only for those boards that support the neon message lamp. Therefore, it is not needed for R1. |
| CLK_HEALTH | Reads the LMM loss-of-clock status bits for the specified tone clock board |
| TDM_NPE_XTALK | Checks if the NPE chip is transmitting on more than one timeslot. Since timeslots are not under the Media server's control, this test will not be run. |
| CONF_TEST | Tests the conference circuit in the NPE. Needs the use of Timeslots; therefore, this test is not run. |
| MOD16_LOOP | A 1004Hz reflective analog loop around on an analog port. This test requires the use of a tone detector and all TDs are under control of the MG. |
| GPP_LP | GPP internal loopback tests is sent through both the I and S channels for a port. A tone detector is needed to detect and report the test pattern. |
| GPP_NPE | The GPP NPE xtalk test. The Media server does not handle network connections, so this test is not run. |
| FT_GPP_LOOP | Factory external loop around test for the GPP board. |
| FT_LOOP | Factory external loop around test for almost all boards. |
| ICSU_LEDS | Checks the Integrated Channel Service Unit LEDs, which do not exist on the DS1 Media Module. |
| DIAL_TONE_TS | Detects dial tone. |
| TRK_AUTO_GRD | This test is for the Australian version of the CO board, TN438. |
| TRK_PPM_TEST | Factory only test for certain CO trunks; requires a pulse generator. |
| TRK_HYB_TS | Tests the loop around capabilities of a port's codec and hybrid circuits. |
| ONS_HYB_TS | Tests the loop around capability on the codec circuit. |
| BRI_EPF | Electronic power feed test; not valid for TN2185. |
| L1_INQ | This function actually encompasses several tests. |
| SSP_TDMLOOP | This is for the messaging angel, but the Media server is unaware of the TDM bus. |
| PRI_TSTCALL | Requires the use of either a data channel or a maintenance test board, neither of which are present. |
| TDMLP_BRI | The Media server can't use the TDM bus. |
| PPP_TDMLOOP | The Media server can't use the TDM bus. |

## Tone detector tests not executed on the G700

Table 26, Tone detector tests not executed on the G700 platform, on page 56 lists the tone detector tests not executed on the G700.

**Table 26: Tone detector tests not executed on the G700 platform**

| Test | Notes |
|---|---|
| TD_DET_TS | The Media server is unaware of the tone detectors, therefore this test does not run. |
| TD_UPD_AUDIT | The Media server is unaware of the tone detectors, therefore this test does not run. |

## Tone generator tests not executed

Table 27, Tone generator tests not executed on the G700, on page 56 lists the tone generator tests not executed on the G700.

**Table 27: Tone generator tests not executed on the G700**

| Test | Notes |
|---|---|
| TG_XTALK_TS | The media server is unaware of the tone generator. |
| TG_XMISSION_TS | The media server is unaware of the tone generator. |
| TG_UPD_AUDIT | The media server is unaware of the tone generator. |

## TDM bus tests not executed on the G700

Table 28, TDM bus tests not executed on the G700 platform, on page 56 lists the TDM bus tests not executed on the G700.

**Table 28: TDM bus tests not executed on the G700 platform**

| Test | Notes |
|---|---|
| TDM_CST_QRY | The Media server is unaware of the TDM bus. |
| TDM_SLP_QRY | The Media server is unaware of the TDM bus. |
| TDM_PPM_QRY | The Media server is unaware of the TDM bus. |
| TDM_CPRUP | The Media server is unaware of the TDM bus. |
| TDM_BD_CH | The Media server is unaware of the TDM bus. |
| TDM_ANLY | The Media server is unaware of the TDM bus. |
| TDM_IDLE_TS | The Media server is unaware of the TDM bus. |
| TDM_BD_IR | The Media server is unaware of the TDM bus. |
| TDM_CC_UPD | The Media server is unaware of the TDM bus. |

## Maintenance features for the G700

Table 29, Maintenance features for Avaya G700 Media Gateway, on page 57 specifies maintenance features as they apply to the Avaya G700 with the S8300 Media Server.

**Table 29: Maintenance features for Avaya G700 Media Gateway**

| Supported feature | Controller S8700/ S8500 S8300 | Notes |
|---|---|---|
| Attendant Console alarm LED and alarm report acknowledgement LED | Yes | Status of G700 alarms is not available on the Attendant Console with a legacy controller. |
| Automatic Trunk Measurement System (ATMS) | No | Not available for analog trunks terminating on a Media Module. |
| DS0 Looparound connection | No | |
| DS1 CPE Loopback | Yes | Test is controlled by the DS1 Media Module. |
| DS1 Synchronization | No | Timing sync is local to the G700 so DS1 sync is controlled by the G700. |
| Enable/Disable Media Module tests | Yes | |
| Enable/Suspend alarm origination | No | Not supported by S8700 platform. |
| Environment tests and alarms for S8300 | | Not available for S8300 in R1. |
| ISDN loop around connection | Yes | |
| ISDN test call | No | Not available for ISDN trunks terminating on a DS1 Media Module. |
| LED tests | Partial | Works with Media Module LEDs but not with the G700 alarm LED. |
| System Configuration Maintenance Object | No | Not needed for Media Module board insertion. Indicates that a board is present but that the board does not respond to a query for board type. |
| System Link test for PRI control link for ISDN DS1 Media Module | No | Layer 2 of a PRI link is terminated in the G700, so this does not apply to the G700 with a S8300 Media Server. A new MO is added for the status and alarming of H.248 links. |

***(1 of 2)***

**Table 29: Maintenance features for Avaya G700 Media Gateway**

| Supported feature | Controller S8700/ S8500 S8300 | Notes |
|---|---|---|
| System tone test call for G700 | No | Requires changes to the call processing software in the S8300 and the G700 |
| TDM Time Slot test call | No | |
| Terminating Trunk Transmission test | No | |
| Test MO command | Yes | Support syntax of Media Module location |
| Test S8300 hardware | Limited | |
| Test of G700 resources:<br>Archangel<br>Network Control Element<br>Packet Interface<br>TDM clock<br>Tone generator<br>Tone detectors | No | Provided by G700 software in a future release. G700 architecture specifies these resources as G700 resources, not S8300 resources. |
| Tests of Media Modules | Partial | Limited by the tests available in R1. |
| Touch Tone Receiver facility test call | No | TTRs in the G700 are not available outside the Media Gateway. |
| Touch Tone Receiver level | No | TTRs in the G700 are not available outside the Media Gateway. |
| Trunk facility test call | Yes | |
| Write Physical Angel command | No | |
| System synchronization | No | |

***(2 of 2)***

# 2 Access and login procedures

This chapter describes the various ways of connecting to, and logging into, the S8300 Media Server and the G700 Media Gateway.

The procedures in this chapter assume that you are connecting to the S8300 and/or the G700 with an Avaya Services laptop. However, the methods apply for any type of PC.

This chapter contains information on these topics:

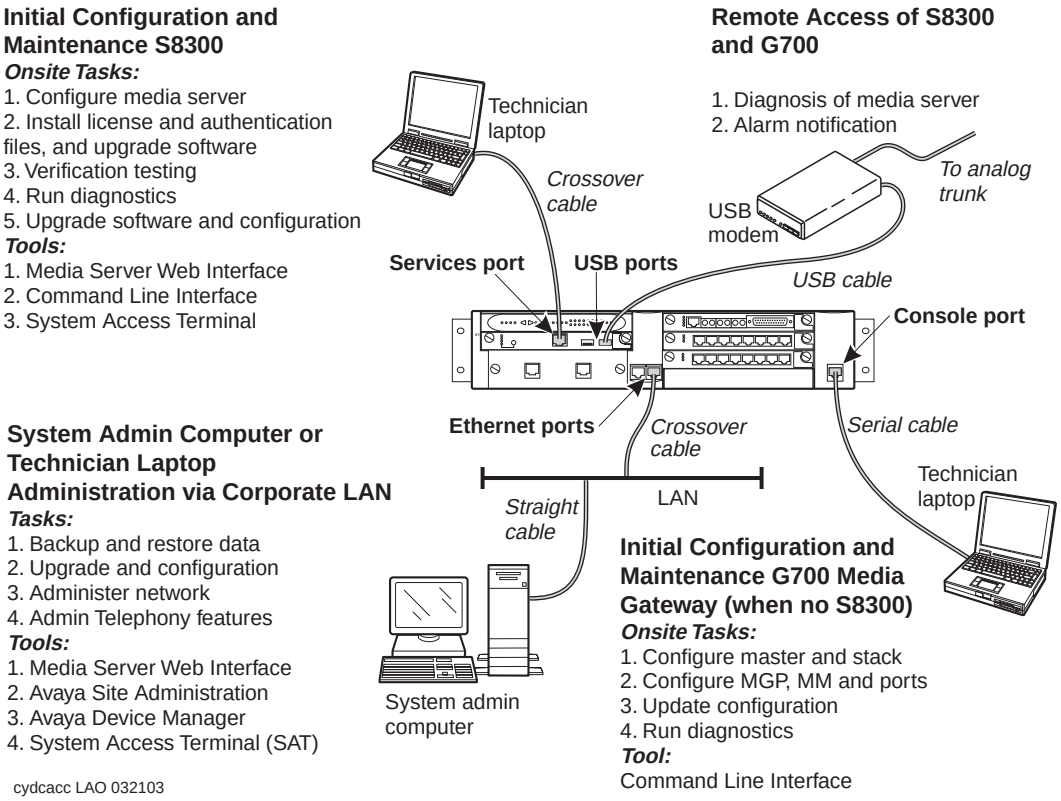


## Connection overview

### *Review physical access methods*

1 Check the Figure 4, Summary of S8300 and G700 access methods and tasks, on page 60 for the location of the S8300 Services port.

**Figure 4: Summary of S8300 and G700 access methods and tasks**




2 If you are providing maintenance for a G700 that does not have an internal S8300, check for the location of the ethernet ports (EXT 1 / EXT 2). You will need to connect the G700 to the customer's LAN through one of these ports.

# Laptop settings and connections

A laptop connected directly to the Services Port on the S8300 Media Server requires specific laptop settings and connections as described in this section.

**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.

- Laptop settings
- Laptop connections

# Laptop settings

On any operating system, the network settings need to reflect the following:

- *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 to locate the correct place to enter this information.

Use these links to go to the two procedures in this section:

- Set TCP/IP properties on Windows systems
- Disable/bypass proxy servers in browser

> **NOTE:**
> 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, try using that profile first before configuring a new one.

## Set TCP/IP properties on Windows systems

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.

### *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.
   - Windows 2000 and XP: change TCP/IP settings on page 61
   - Windows 95, 98, NT 4.0, and ME: change TCP/IP properties on page 62

### *Windows 2000 and XP: change TCP/IP settings*

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 might need to restore them later to connect to another network.

8 **Disable DNS service as follows:**

1 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.

2 Click the **Advanced** button at the bottom of the screen. The ***Advanced TCP/IP Settings*** screen appears.

3 Click the **DNS** tab and verify that no DNS server is administered (the **Address** field should be blank).

9 Disable WINS Resolution as follows:

1 Click the **WINS** tab. Make sure WINS is not administered (the **Address** field should be blank).

2 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.

### *Windows 95, 98, NT 4.0, and ME: change TCP/IP properties*

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 checkbox 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.

## 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 **OK** 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.

# Laptop connections

***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 the Table 30, Crossover cable pinout chart, on page 65 for pinout connections if needed. Crossover of the transmit and receive pairs (as shown) is required.

**Table 30: Crossover cable pinout chart**

| Pin to 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**

## Connecting through the G700 serial port

To configure a G700 that *does not have an S8300*, you might need to set up a direct connection from your laptop's serial port to the G700 Console (serial) port.

### *To connect a laptop directly to the serial port on the G700 Media Gateway:*

1 For a stacked configuration, locate the device that contains the master controller for the stack. Check the LED panel on the upper left of each G700 or P330 device in the stack as follows:

- G700 Media Gateway: a lit **MSTR** LED indicates that this unit is the stack master.
- A non-G700 P330 device: a lit **SYS** LED indicates that this unit is the stack master.

2 Connect the RS-232 serial cable and DB-9 adapter cable provided with the G700 between your laptop and the G700:

- Attach one end of the RS-232 cable to the RJ-45 jack on the front of the G700 that is the stack master. The serial port is on the lower right side of the chassis, 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.

3 Use a serial-connection program such as HyperTerminal to access the P330 stack processor.

## Connecting through the LAN

To connect to the customer's LAN, either on site or remotely over the Internet, your laptop 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.

# Connecting through an external modem

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 Logging in to the S8300 Web interface from your laptop on page 72), and click Enable/Disable Modem on the main menu

   The system displays the Enable/Disable 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 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 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 Use Windows for modem connection to the Media Server (Windows 2000 or XP) on page 66.

> **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** checkbox.

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 Uncheck (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 through a 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 Avaya Integrated Management. 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 dragdown 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 Logging in to Communication Manager (SAT screens) on page 76.

## 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 dragdown 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 dragdown 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 **9500** from the dragdown 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 Logging in to Communication Manager (SAT screens) on page 76.

## Terminal emulation function keys

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 31, ntt terminal emulation function keys, on page 70 as a guide for **ntt** terminal emulation.

**Table 31: 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 32, w2ktt terminal emulation function keys, on page 71 lists key presses for **w2ktt** terminal emulation.

**Table 32: 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 |

# Login methods

This section describes how to log on to the S8300 Media Server using Telnet or the built-in Web Interface and how to start a SAT session. These procedures assume that:

- You have a crossover cable directly connected from you 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 procedures in this section include:

- Logging in using a telnet session on your laptop
- Logging in to the S8300 Web interface from your laptop
- Logging in to Communication Manager (SAT screens)
- Logging in to the Layer-2 switching processor

The last procedure in this section describes logging in to the Layer 2 Switching processor when you have a direct serial connection to the G700 Console port.

## Logging in using a telnet session on your laptop

### *To run telnet*

1. Ensure you have an active Ethernet or serial connection from your computer to the 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*>.

## Logging in to the S8300 Web interface from your laptop

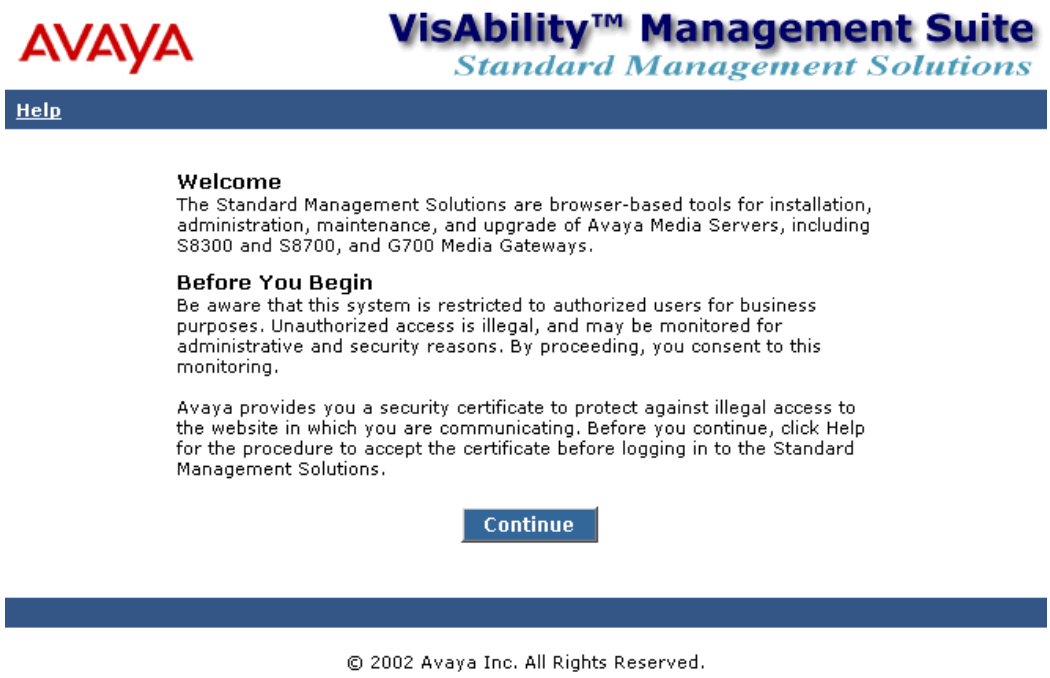
### *To run the Web Interface*

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 Welcome screen (Figure 5, Welcome screen, on page 73) displays.

**Figure 5: Welcome screen**

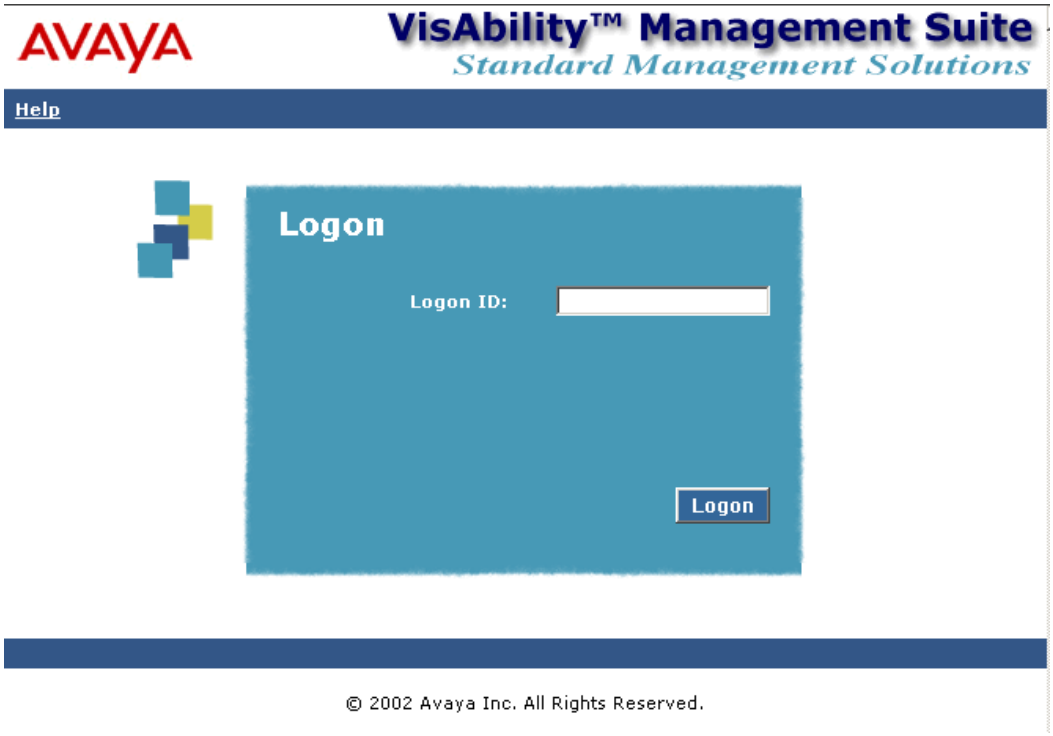



3 Click the **Continue** button.

4 Accept the server security certificate to access the Login screen.

The Login screen (Figure 6, Logon screen, on page 74) displays.

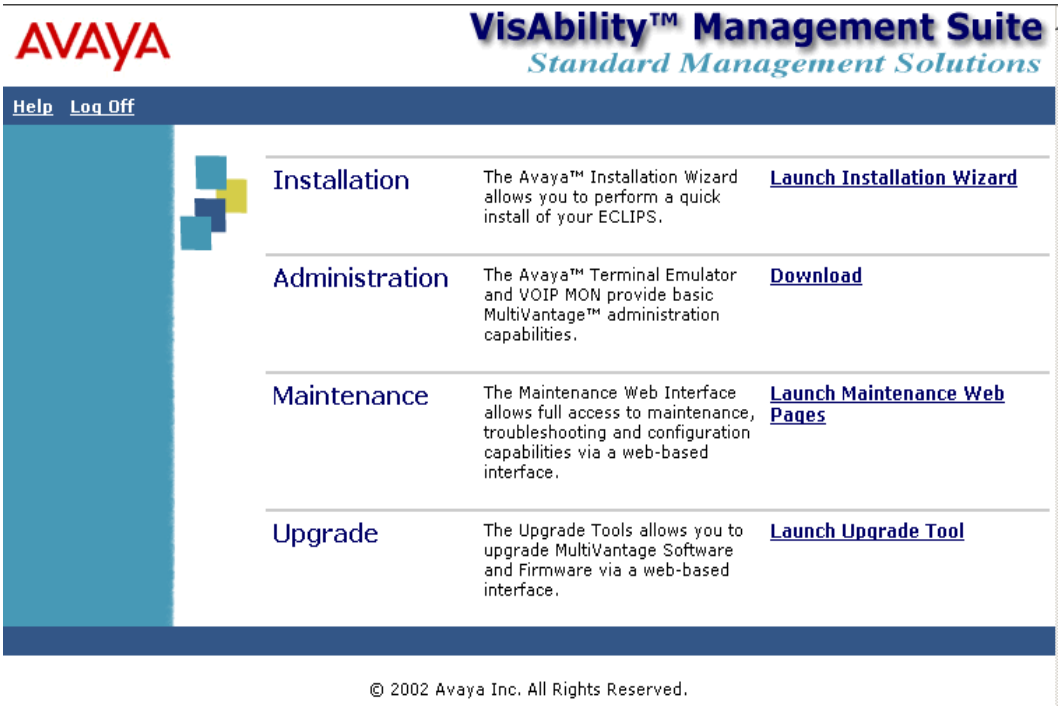
**Figure 6: Logon screen**




5 Log in as **craft**.

The main menu (Figure 7, Main menu, on page 75) displays.

**Figure 7: Main menu**




**6** Click on the link for **Launch Maintenance Web Pages**

The system displays the S8300 main menu in the left panel and a usage-agreement notice in the right window (Figure 8, Maintenance Web pages, on page 76).

**Figure 8: Maintenance Web pages**


7 Check the top of the left panel.

- The Avaya Media Server you are logged into is identified by name and server number.
- The S8300 Media Server number is always 1.

## Logging in to 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.

# Logging in to the Layer-2 switching processor

Use one of the following procedures, depending on your means of connection:

- Direct connection to the Services port
- LAN connection
- Direct serial connection
- Access through Device Manager

## Direct connection to the Services port

Use this procedure to log in to the Layer 2 Switching Processor when you have a direct connection with your laptop to the S8300 Services port.

### *To log in to the Layer 2 Switching Processor via the Services port*

**NOTE:**
If you are upgrading an S8300/G700 remotely, connect to the customer LAN and telnet to the IP address of the Layer 2 stack master (that is, the P330 stack processor running as the stack master). The IP address is the address assigned on the customer LAN, not 192.11.13.6.

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 stack master processor.

Type **`telnet <xxx.xxx.xxx.xxx>`**, where `<xxx.xxx.xxx.xxx>` is the IP address of the Layer 2 stack master processor on the customer's LAN.

4 Login at the Welcome to Avaya P330 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 `P330-1(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:

`P330-1(super)#>` **`set help`**

you will be given the current list of **`set`** commands available. If you type:

`P330-1(super)#>` **`set interface help`**

you will be given a much more restricted list of command possibilities that address the possible interfaces to be set.

For a complete list of command line interface commands, type **`help`** or refer to the *Avaya P330 Manager User Guide.*

## LAN connection

Use this procedure to log in to the Layer 2 Switching Processor when you have a connection to the customer's LAN.

### *To log in to the Layer 2 Switching Processor with a LAN connection*

1. With a connection to the customer's LAN (either remotely or on site), telnet to the P330 stack processor IP address:

   Type **`telnet <xxx.xxx.xxx.xxx>`**, where `<xxx.xxx.xxx.xxx>` is the IP address of the P330 stack master processor on the customer's LAN.

2. Login at the Welcome to Avaya P330 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 `P330-1(super)#`.

## Direct serial connection

Use this procedure to access the G700 processors when your laptop is directly connected to the S8300 Console port through a serial cable.

### *To access the G700 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 P330** 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 `P330-1(super)#`.

## Access through Device Manager

To access the Device Manager, you must have access to the corporate LAN in which the Layer 2 Switching Processor resides.

***To access 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 1.2.2 or 1.3.1 is required.
2. In the Address (or Location) field of your browser, type the IP address or name of the Layer 2 Switching Processor 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://P330-stack1.mycompany.com`

     **NOTE:**
     The Device Manager is *not* available through the S8300 Media Server. You must be connected to either the Layer 2 Switching Processor or G700 Media Gateway processor through the corporate LAN.
3. A GUI rendering of the stack devices appears. Proceed with Media Gateway or stack device administration.

# Logins and passwords on the S8100

This section describes passwords and logins on the S8100 system.

This chapter provides information about the setup and use of customer logins:



## Customer access

In S8100, the Lucent Access Control (LAC) module allows access to a "shell" (also called "bash") using any valid Windows 2000 login. This enhancement allows a customer to use a login, such as NTADMIN, to access Windows 2000 via a "bash shell". This feature is not intended to be used by Avaya Services personnel who continue to use the Lucent Services logins (lucent1, lucent2, lucent3).

In S8100, the LAC module listened only on TCP port 23. A connection to this port produced different results depending on the login used. For example, a services login (lucent1, lucent2, lucent3) resulted in the "lac" prompt to select Communication Manager, INTUITY AUDIX, or a Bash shell. An alias login, such as dinit, resulted in a Communication Manager SAT screen without a LAC prompt. This continues to be supported in S8100, but is being deprecated in favor of the use of separate telnet ports for direct access to Communication Manager and INTUITY AUDIX.

If the telnet session is established to TCP port 22, and the login has privileges to access Communication Manager, a connection is made directly to a Communication Manager SAT without a LAC prompt. If the caller logs off, the telnet session is terminated.

If the telnet session is established to TCP port 24, and the login has privileges to access INTUITY AUDIX, a connection is made directly to an INTUITY AUDIX Forms Controller administration screen without a LAC prompt. If the caller logs off, the telnet session is terminated.

The same logins are used with ports 22, and 24, as well as 23. The difference is that a direct connection is made to the appropriate application without a LAC prompt or having to use an alias login.

See "Avaya Site Administration" in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

## Windows 2000 logins for the customer

Several Windows 2000 login groups and associated passwords are pre-installed for customer use from the factory. See Table 33, Windows 2000 logins, on page 80.

The login IDs in the last two columns of Table 33, Windows 2000 logins, on page 80 are for customer use. The following describes use and administration of these logins.

**Table 33: Windows 2000 logins**

| | Logins for customer use | |
|---|---|---|
| **Windows 2000 logins** | **User name** | **Default password** |
| Administrators | NTadmin | NTadmin1 |
| Guest - disabled | -- | -- |
| lucent | -- | -- |
| officeadmin | [1] | |
| officeuser | [2] | |
| Power Users | -- | -- |
| Users | browse<br>vm<br>sa | |

1 To be administered

2 To be administered

**WARNING:**

The logins in the lucent group of Table 33, Windows 2000 logins, on page 80 are for the exclusive use of Avaya Services personnel. These logins are established and updated automatically by Avaya software. DO NOT ALTER THESE LOGINS IN ANY MANNER. To do so may render the system unserviceable and may require a partial or complete reinstallation of the software by Lucent personnel.

# Windows 2000 login types for the customer

## Administrator login

- **NTadmin**

  This is a standard Windows 2000 administrator account used to administer network parameters and similar functions.

## INTUITY AUDIX logins

- **browse**

  This login is used in the Voice Messaging application. See the INTUITY AUDIX documentation or Table 34, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 81 for a list of commands accessible to the browse login. This login is disabled from the factory. It must be enabled and a password chosen before it can be used.

- **vm**

  This login is used in the Voice Messaging application. See the INTUITY AUDIX documentation or Table 34, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 81 for a list of commands accessible to the vm login. This login is disabled from the factory. It must be enabled and a password chosen before it can be used.

- sa

  This login is used in the Voice Messaging application. It has full customer administration privileges. See the INTUITY AUDIX documentation or Table 34, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 81 for a list of commands accessible to this login. This login is disabled from the factory. It must be enabled and a password chosen before it can be used.

  **NOTE:**
  The stand-alone INTUITY AUDIX system login **sa** normally produces a menu. This feature is not supported on an S8100. All logins result in a Forms Screen interface.

**Table 34: INTUITY AUDIX commands versus logins for sa, vm, and browse**

| Command | Login | | |
|---|---|---|---|
| | sa | vm | browse |
| add | 3 | 3 | |
| audit | 3 | 3 | |
| change | 3 | 3 | |
| copy | 3 | | |
| display | 3 | 3 | 3 |
| exit | 3 | 3 | 3 |
| get | 3 | 3 | |
| help | 3 | 3 | 3 |
| list | 3 | 3 | 3 |

*(1 of 2)*

**Table 34: INTUITY AUDIX commands versus logins for sa, vm, and browse**

| Command | Login | | |
|---|---|---|---|
| | sa | vm | browse |
| logoff | 3 | 3 | 3 |
| print | 3 | 3 | 3 |
| remove | 3 | 3 | |
| reset | 3 | | |
| test | 3 | 3 | 3 |
| toggle | 3 | 3 | 3 |
| trace | 3 | 3 | 3 |

*(2 of 2)*

### Customer Web access logins

The following login groups are used for web access:

- Officeadmin

  Login IDs in this group are installed from the factory. This login group facilitates access via the S8100 web interface. Group members select administrative privileges via the web interface. The NTadmin account is used to establish an account in this group. Generally, an account in the **Officeadmin** group is used to download Avaya Site Administration from the S8100 Web page.

- Officeuser

  Login IDs in this group are installed from the factory. This login facilitates download of client software, such as Message Manager. Group members have access for client download only. The NTadmin account is used to establish an account in this group. An **Officeuser** group account is generally used to download Message Manager from the S8100 Web page.

- **anonymous**

  The **anonymous** login is for very limited access via the web interface to load a software patch.

## Enabling Windows 2000 customer logins

Only the Administrator can enable customer logins.

### Setup login accounts

1. Start the Windows 2000 user manager on the S8100 desktop. Click **Start > Programs > Administrative Tools > User Manager**
2. Change the password for the **NTadmin** account.
3. Activate and set passwords for the **browse**, **vm**, and **sa** accounts. This also can be done via the command line tool **net user**. See “Lucent access controller bash commands” in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*

4 Create three Windows 2000 accounts in the Officeadmin group for three application administrators. These accounts are used to download ASA software. The account names can be chosen as desired. For this example they are called D1user1, D1user2, and D1user3.

5 Create one Windows 2000 account in the Officeuser group for download of the INTUITY Message Manager Software.The NTadmin account should be used for Windows 2000 administration only. The account name can be chosen as desired. For this example it is called D1WEB.

**NOTE:**
The **NTadmin** account can be used for download, but should be used for Windows 2000 administration only.

## Communication Manager logins for the customer

In addition to the logins maintained in the Windows operating system, there are customer level logins within the Communication Manager application that do NOT appear as Windows logins. The default password should be changed by the customer during installation.

**Table 35: Communication Manager customer logins**

| Communication Manager customer logins | Comments | Default password |
|---|---|---|
| defty1 | This is the customer level “super user” login within the Communication Manager application. Its use should be restricted to the system administrator. This login can be used to create additional Communication Manager logins. See the Communication Manager command **add login**. | |

S8100 provides enhanced login/password security by adding a security feature that allows users to define their own Communication Manager logins/passwords and to specify a set of commands for each login.

- The system allows up to 14 simultaneous connections (logins) to Communication Manager. (Communication Manager can have 5 connections, INTUITY AUDIX can have 4 connections, and the rest of the connections are reserved for shell commands.)
- Each S8100 login name can be customized.
  - — Logins must be 3 to 6 alphabetic/numeric characters, or a combination of both.
  - — A password must be from 4 to 11 characters in length and contain at least 1 alphabetic and 1 numeric symbol.

Password aging is an optional feature that the super-user administering the logins can activate (see below).

**NOTE:**
If several users are logging in and out at the same time, a user may see the message: `Transient command conflict detected; please try later`. After the “users” have completed logging in or out, the terminal is available for use.

## Forced password aging (Communication Manager-specific)

Forced password aging operates as follows:

1. The password for each login can be aged starting with the date the password was created, or changed, and continuing for a specified number of days (1 to 99).
2. 7 days before the password expiration date, the user is notified that the password is about to expire at the login prompt.
3. When the password expires the user is required to enter a new password into the system before logging in.
4. If a login is added or removed, the "Security Measurement" reports are not updated until the next hourly poll, or a **clear measurements security-violations** command is entered.
5. Once a non-super-user has changed the password, the user must wait 24 hours to change the password again.

## Logoff notification (Communication Manager-specific)

Security is enhanced by providing a logoff notification screen to a system administrator at log off while either the facility test call or remote access features are still administered. The administrator can be required to acknowledge the notification before completing the logoff process. Logoff notification is administered on the Login Administration screen.

## Super-User

S8100 is delivered to the customer with one customer "super-user" login/password defined. The customer is required to administer additional login/passwords as needed. The super-user login has full customer permissions and can customize any login created.

Login permissions for a specified login can be set by the super-user to block any object that may compromise switch security. Up to 40 administration or Administer Trunks

- Additional Restrictions
- Administer Features
- Administer Permissions

- Maintenance Commands

  **NOTE:**
  Enable MSP features using **change system-parameters customer-options**.

  - Maintain Stations
  - Maintain Trunks
  - Maintain Systems
  - Maintain Switch Circuit Packs

## Administer login command permissions

Users with super-user permissions can set the permissions of logins they create by performing a **change permissions <login-name>** command. This causes the Login Permissions form to display. The Login Permissions form allows the user to control access to various categories of commands for a given login. It also permits restricting access to objects (forms) on an individual basis for up to 40 objects. Restricting an object means that no commands may be performed on that object by that login (add, change, remove, etc.) The three main categories of commands are:

- Common Command
- Administration Commands
- Optional Maintenance Commands

Each category of commands has sub-categories that, when set to **y,** allow access to objects associated with that sub-category. If the category is set to **n**, the user is not be able to add, remove, or change commands on objects under that sub-category. If the display category is **y**, the login will list or display the object in most cases. If the super-user wants to restrict access to all commands associated with an individual object in a subcategory, the `Additional Restrictions` field is set to **y**. This causes 2 additional pages to be added to the Permissions form. Scroll these pages and press **Help**. Individual objects will be displayed in alphabetical order. Enter the object that you want to restrict access to into the fields and submit the form. Up to 40 objects may be restricted. A restricted login cannot access any of the commands associated with that login. Note that permissions cannot be changed for the login and you cannot create Additional Restrictions without full super-user permissions.

## Password expiration

If your password has expired, the following message displays:

**Figure 9: Password expiration screen**

```
          Login: telmgr

       Password:
       Your Password has expired, enter a new one.

   Reenter Current Password:

               New Password:

       Reenter New Password:
```

If your password is within 7 days of the expiration date, the following message displays:

```
WARNING: Your password will expire in X days
```

# Avaya Site Administration configuration

You can usually download Avaya Site Administration from the Media Server Home Page (select **Download** next to Administration). Then follow the directions presented by the download/installation wizard.

The procedures in this section include

- Adding a switch connection
- Logging in to the server

### *Adding a switch connection*

After Avaya Site Administration is installed, it must be configured to communicate with Communication Manager on the S8300 Media Server. This is done by creating a new switch connection entry:

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, ALWAYS use port **23** for the *craft* login; use port **5023** for the customer login.

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 server*

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.

1. To start Avaya Site Administration, click **Start** > **Programs** > **Avaya** > **Site Administration**.

2. Select the server that you want to access.

3 When prompted, log in.

4 When you are logged in, click **Start GEDI**.

# Navigating the Command Line Interface

Table 36, Navigational aid for CLI commands, on page 87 describes a few Command Line Interface commands that you will need to navigate between the processors on the G700.

Log in to the Layer 2 Switching processor. Default mode is "Supervisor" with a P330-1(super)# command-line prompt.

**Table 36: Navigational aid for CLI commands**

| Command | Purpose | Prompt |
|---|---|---|
| super | change to supervisor mode | `P330-1(super)#` or `<MG name>-1(super)#` |
| configure | change to configuration mode | `P330-1(configure)#` or `<MG name>-1(configure)#` |
| session <*module #*> mgp (from a stack processor session) | open a CLI session on the mgp processor | <*MG name*>-1(super)# |
| session <*module #*> stack (from an MGP session) | open a CLI session on the stack processor | P330-1(super)# |
| session *i*cc (from an MGP session) | open a CLI session on the S8300 processor | craft@<*host name*>> |
| **`session <#>`** | open a session on the stack processor in module (i.e. another G700)<#> in the stack | P330-<#>(super)# |
| **`exit`** | close the current session (and revert to the previous session) | |
| `<command>` help | displays help for `<command>` | |

The command-line prompts in an MGP session use the media gateway's name that is assigned when it is configured.

You can telnet to another processor from a current telnet session.

**S8100**

# Accessing the S8100 Media Server for maintenance

There are several ways to connect to the S8100 system:

- Web browser interface on page 88
- Telnet session on page 88
- Avaya site administration on page 89

This section describes these types of interfaces and when it is appropriate to use them. For more information, see Chapter 2, “Connectivity and Access to S8100” in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146.*

## Web browser interface

You can perform these basic maintenance and administration functions on the S8100 from a standard web browser (such as Internet Explorer):

- Backup
- Restore
- Restart
- Download software
  - — Avaya Site Administration
  - — INTUITY Message Manager

To use the web browser interface, see “Via a Web browser session” in Chapter 2, “Connectivity and Access to S8100” in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146.*

## Telnet session

Opening a Telnet session to the S8100 system allows you to:

- Open a command line interface
- Run the INTUITY AUDIX administration application

The Telnet session provides access to all areas of S8100 maintenance and administration.

You will need special permissions to open a Telnet session to the S8100. Access requires an encrypted response to a login challenge.

### Command line interface

The command line interface is available in the UNIX bash shell using the **bash** command. The bash shell accepts the Global Administration Subsystem (GAS) commands that are listed in *Maintenance Commands Reference (555-245-101)*. Use this interface to:

- Reset system
- Shutdown system
- Install License and Authentication files

> **NOTE:**
> Refer to the *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*, Chapter 3, System Initialization, Section, “Obtaining a License.”

- Startup/shutdown system IP addresses
- Enable Individual application (or process)
- Verify system alarm status
- Display and clear global alarms
- Turn global alarm reporting of INADS on and off
- Verify software versions

### Communication Manager SAT

The Communication Manager SAT screens are enabled from a Telnet session. This acts in the same manner as a SAT terminal connected to any other Communication Manager system.

### INTUITY AUDIX application

For a laptop, you can run the command line INTUITY AUDIX application, using the AUDIX command.

## Avaya site administration

Opening an Avaya Site Administration session provides access to all areas of S8100 maintenance and administration. Avaya Site Administration performs most of the switch administration activities (except for monitor commands). In Avaya Site Administration you can:

- Start the session as a normal application from Windows at the start button
- Enable your browser

The Avaya Services representative uses the logins **Lucent1**, **Lucent2**, or **Lucent3** and the Windows 2000 password/ASG challenge.

# 3 License and Authentication files

This chapter describes how to install License and Authentication files on the following equipment:

- Avaya S8700 Media Server
- Avaya S8500 Media Server
- G700 Media Gateway (controlled by an Avaya Media Server).

The procedures contained in this chapter do no explain the function of the License or Authentication files; for more detailed information these files, refer to *Administrator's Guide for Avaya Communication Manager, 555-233-506*.

## Installing License and Authentication files

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. The License File is reinstalled to add or remove call-processing features. 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 Authentication file can be installed independently of each other or any other server upgrades.

### Downloading the License and Authentication files

Use the License File Remote Feature Activation (RFA) to obtain the License and Authentication files. 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, 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, download the License and Authentication files to the services laptop.

To access the RFA application, you must take the RFA online training and pass the online test.

### RFA information requirements (new installations)

You need the following information before going to the RFA website:

- Your personal Single Sign-On (SSO) for RFA website authentication login.
- SAP order number
- Required customer information
- Serial number of one of the TN2312 IP server interface (IPSI) circuit packs chosen to be the reference IPSI for the license.
- 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 Website

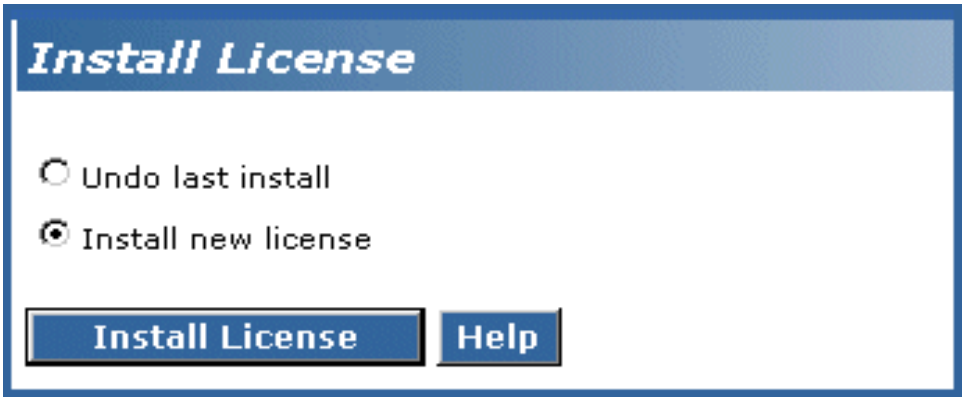
The RFA website automates some of the installation procedures, including generating license and Avaya authentication files. Go to http://rfa.avaya.com.

## Installing License and Authentication Files

***To install the License and Authentication files***

1 Under **Security** click **Install License,** select “Install new license,” then click the Install License button to install the License Files.

**Figure 10: Install license**




After you install the License File, the server will be in No License Mode until it recognizes the reference G700 (the G700 in which the S8300 or LSP is physically inserted), which is after it receives its IP address later in the process. This is normal on a new installation.

Installing the 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.

2 Click **Install Avaya Authentication** > **Install** to install the Authentication File.

# License Files for different configurations

License files are assigned differently, depending on the Media Server and G700 Media Gateway configuration.

## S8300 Media Server

When the system configuration is a G700 with an S8300, the S8300 is a Linux-based processor running Communication Manager. The serial number of the G700 in which the S8300 is inserted is used in the License File for identification.

## S8700 Media Server

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 G700 does not require a separate License File and is thought of as an extension of the server's platform. Licensing is handled by the S8700 Media Server.

## Survivable configuration

In a survivable configuration, the S8300 Media Server is configured as a Local Survivable Processor (LSP). The LSP is present on the G700, 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 G700 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 G700 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.

The Local Survivable Processor field in the *OPTIONAL FEATURES* section of the Customer Options form indicates that the switch is an S8300 functioning in Local Survivable Processor mode. This field is modified only through the License File and is “display only” on the Customer Options form.

# License File modes

License files for the Avaya S8300 Media Server in an Avaya G700 Media Gateway function in the following three modes:

## License-Normal

This is the desired mode of operation for a stable switch. In this mode, a license is properly installed, the license contains a serial number that matches the G700’s, the license is not expired, and the feature usage does not exceed limits set in the license.

## License-Error

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 G700 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

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 two types of entries in the feature mask:

- Type I Entry
- Type II Entry

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 37, Type I Feature License Behavior, on page 95.

**Table 37: Type I Feature License Behavior**

| License content | | Consequence | |
|---|---|---|---|
| **Value** | **Lock** | **Feature status** | **Options[1] screen** |
| On | Unlocked | Set by translation via login. If no translation, feature is enabled. | init and dadmin can administer this feature. |

*(1 of 2)*

**Table 37: Type I Feature License Behavior**

| License content | | Consequence | |
|---|---|---|---|
| **Value** | **Lock** | **Feature status** | **Options[1] screen** |
| 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, that is the login affects the 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. |

*(2 of 2)*

1 Offer-options, customer-options, and special applications forms.

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 38, Type II and Type III feature License File behavior, on page 96.

**Table 38: Type II and Type III feature License File behavior**

| License content | Consequence | |
|---|---|---|
| **V1 and V2** | **Feature status** | **Options[1] 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. |

1 Offer-options, customer-options, and special applications forms.

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 38, Type II and Type III feature License File behavior, on page 96.

# 4 Hardware configurations

This chapter includes the following topics:



## Multicarrier cabinets

For information on the MCC1 (multicarrier) cabinet and the carriers in them, refer to *Hardware Guide for Avaya Communication Manager, 555-233-200.*

## PNC cabling — fiber-optic hardware

The term “fiber” is used to refer to all the hardware needed for the three basic types of connections used to form multi-PN systems:

- EI-to-EI or EI-to-SNI intercabinet hardware
- EI-to-SNI or EI-to-EI intracabinet hardware
- EI-DS1CONV or SNI-DS1CONV hardware

The term “fiber administration” specifies the

- Endpoints that are connected.
- Optional DS1 CONV locations.
- Parameters for DS1 facility line encoding and equalization.

The connection types discussed in this section are

- EI-to-EI or EI-to-SNI intercabinet fiber-optic cables
- EI-to-SNI or EI-to-EI intracabinet metallic cabling
- DS1 CONV cabling

### EI-to-EI or EI-to-SNI intercabinet fiber-optic cables

EI-to-EI or EI-to-SNI intercabinet connections are implemented by installing a lightwave transceiver on the I/O connector plate for each of the administered fiber endpoints. Each lightwave transceiver has a receive and a transmit connector for either a 62.5-micron or 50-micron fiber connection. Standard fibers

are available in various lengths up to 150 feet (46 m) for single-mode fiber and up to 200 feet (61 m) for multimode fiber. These fibers are used to connect lightwave transceivers to each other when they are close enough together, or to optical cross-connect facilities for greater distances.

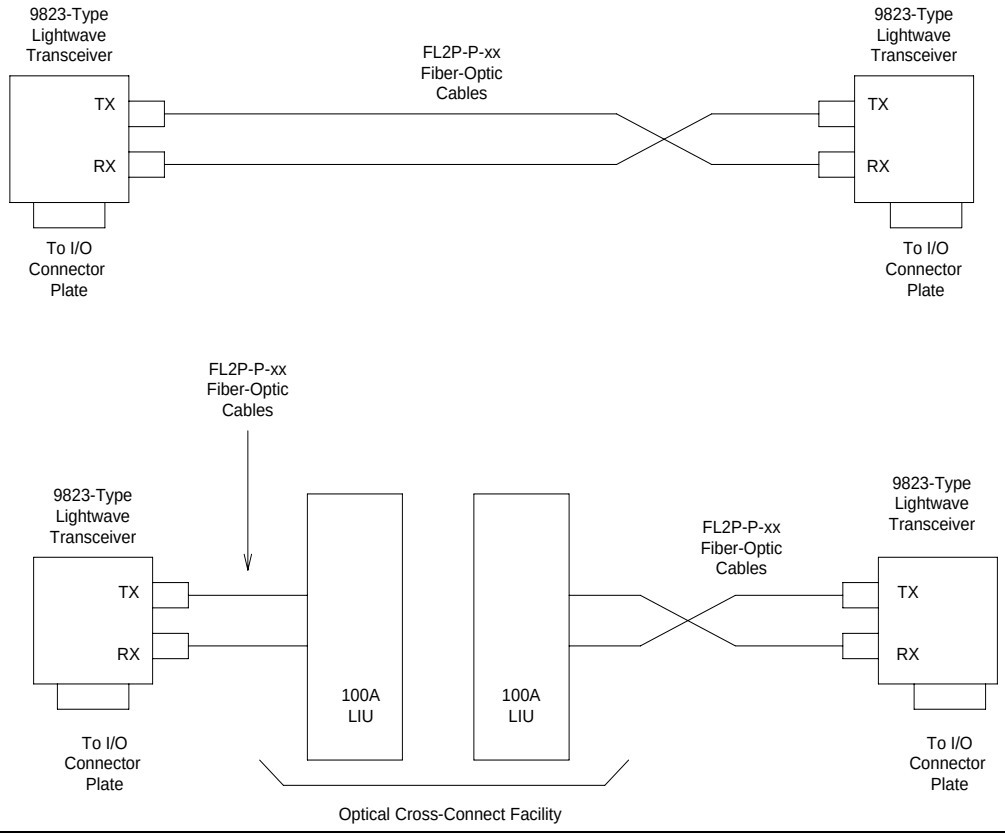
The lightwave transceivers are powered from I/O connector plate leads attached to TN570 Expansion Interface circuit pack or a TN573 SNI circuit pack. The transceivers include loop-around capabilities to support fiber fault isolation. Table 39, Lightwave transceiver specifications, on page 98 lists part number and distance specifications for the two length-dependent 9823-type multimode transceivers and the 300A single mode fiber transceiver. The transceivers at each end of the fiber should match.

**Table 39: Lightwave transceiver specifications**

| Lightwave transceiver part number | Maximum fiber length | Fiber mode |
|---|---|---|
| 9823A | 4900 feet (1494 m) | Multimode |
| 9823B | 25,000 feet (7620 m) | Multimode |
| 300A | 22 miles (35.4 km) | Single mode |

Figure 11, Fiber link connection hardware, on page 98 illustrates the interconnection of fiber-optic hardware.

**Figure 11: Fiber link connection hardware**



## EI-to-SNI or EI-to-EI intracabinet metallic cabling

Metallic cable can be substituted for fiber-optic cable for “fiber” connections between EIs or between an EI and an SNI in the same MCC cabinet, using the same I/O plate connectors.

**DANGER:**
**The metallic cables should not be used for intercabinet connections, since doing so would violate system ground integrity.**

Table 40, Metallic cable specifications, on page 99 lists the part numbers and uses for the two (2) metallic cable lengths.

**Table 40: Metallic cable specifications**

| Metallic cable part numbers | Length | Use |
|---|---|---|
| H600-278,G1 | 13 inches (33 cm) | From an EI in slot 1 of a switch node carrier to an SNI in the same half of the carrier (usually the adjacent slot) |
| H600-278,G2 | 66 inches (168 cm) | From an EI to an SNI in the same cabinet, but in a different carrier or different half of a carrier |

## DS1 CONV cabling

When fiber-optic cabling is not practical, Digital Service 1 (DS1) can be used to connect PNs up to 100 miles (161 km) apart. A TN574 or TN1654 DS1 Converter (DS1 CONV) circuit pack serves as the interface between the network and an EI or SNI on the switch. DS1 cabling on a carrier consists of a Y-cable that connects a DS1 CONV to an EI or SNI and to the network. Table 41, DS1 CONV cable specifications, on page 99 lists the lengths and uses for DS1 CONV cables, depending upon where the DS1 CONV and the EI or SNI are located.

**Table 41: DS1 CONV cable specifications**

| Connection location | Length | Comcode (TN574) | Comcode (TN1654) |
|---|---|---|---|
| On same half carrier | 1 foot (30.48 cm) | 846448637 | 847245750 |
| On different half carriers in same cabinet | 5.5 feet (1.68 m) | 846448645 | 847245768 |
| Between two adjacent cabinets | 1 foot (30.48 cm), used with two 9823As, and 1 20-foot (6.1-m) fiber-optic cable | 846448652, and one 846885259 bracket | 847245776 with one 846885259 bracket |

The DS1 CONV to EI/SNI cable is a shielded metallic Y-cable held in place at the EI/SNI port connector by a 4B retainer and at the DS1 CONV port connector by a 4C retainer. The cable end with one 25-pair amphenol connector attaches to the I/O Plate connector for the EI or SNI. The end with two 25-pair amphenol connectors attaches to the DS1 CONV I/O plate connector.

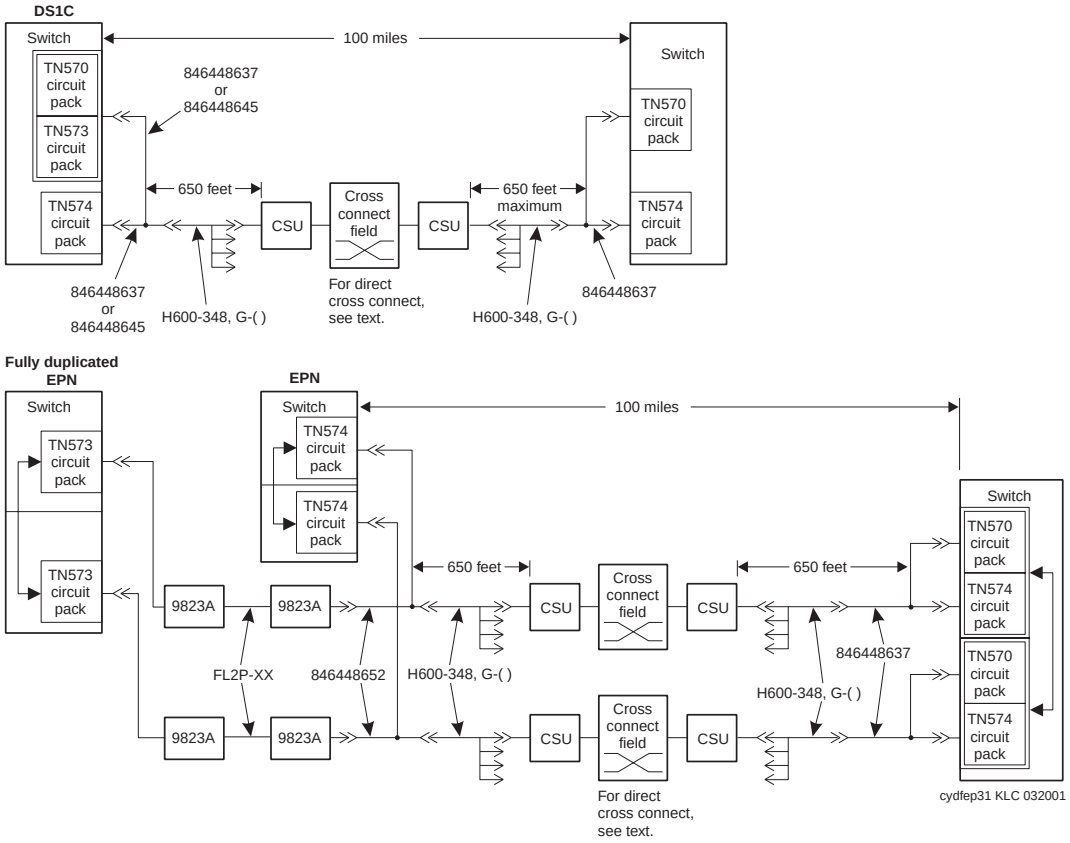
The 13-inch cable 846448652 or 847245776 connects the DS1 CONV to a fiber-optic cable, enabling the DS1 CONV to connect to an EI or SNI at a greater distance. The cable end with one 25-pair amphenol connector attaches to a lightwave transceiver using the 846885259 bracket. The end with two 25-pair amphenol connectors attaches to the DS1 CONV I/O plate connector. The other end of the fiber-optic cable connects to a lightwave transceiver attached to the I/O plate connector of the EI or SNI.

An H600-348 cable connects the DS1 CONV cable to a CSU (channel service unit), which connects to a wall field (Figure 12, DS1 CONV connections to remote PNs, on page 101). Alternatively, connection is sometimes made directly from the Y-cable to the wall field (see the pinout for the 50-pin connector at the end of the section titled Fiber link fault isolation on page 167). This cable provides from one to four DS1 connections. One end of the H600-348 cable is plugged into the 50-pin amphenol piggy-back connector on the 8464486xx cable connected to the DS1 CONV port connector. The other end of the H600-348 cable has four 15-pin sub-miniature D-type connectors that plug into the CSU (see pinout at the end of the Fiber link fault isolation on page 167 section). Table 42, H600-348 cable specifications, on page 100 lists the H600-348 cable specifications.

**Table 42: H600-348 cable specifications**

| Group No. | Length | Group No. | Length |
|---|---|---|---|
| G1 | 25 feet (7.62 m) | G5 | 125 feet (38.1 m) |
| G2 | 50 feet (15.24 m) | G6 | 200 feet (60.96 m) |
| G3 | 75 feet (22.86 m) | G7 | 400 feet (121.9 m) |
| G4 | 100 feet (30.48 m) | G8 | 650 feet (198 m) |

**Figure 12: DS1 CONV connections to remote PNs**




1 Place duplicate pairs in different carriers.

2 When removing two or more, the maximum cable distance between any two remoted endpoints is 100 miles (161 km). For example, if one PN is 75 miles (121 km) from the switch node cabinet, then no other PN can be more than 25 miles (40.2 km) from the same switch node cabinet.

3 Use a 846447637 within a carrier for a TN574, use a 847245750 within a carrier for a TN1654.

Use a 846448645 within a cabinet between carriers for a TN574, use a 847245768 within a cabinet between carriers for TN1654.

# Circuit packs

Check the Minimum Vintage Table to determine which circuit packs will work with the Avaya S8700 Media Server for Multi-Connect Configuration. This table can be found online at http://support.avaya.com (search for “Minimum Vintage Table”) or in the Software Release Letter that accompanies the software CD.

Refer to *Hardware Guide for Avaya Communication Manager, 555-233-200* for more information on supported circuit packs.

# Duplication for reliability

### S8700 only

The S8700 has duplicated components to increase the reliability of the system. If one duplicated component fails, the other can take over without impacting service or minimizing the impact. Which components are duplicated in your system depends on the level of reliability chosen for your configuration: duplex, high, or critical reliability. Consult the following sections for descriptions of these different reliability levels and their configurations:

- Standard and High Reliability configurations
- Critical Reliability configuration

The S8700 IP Connect architecture has duplex reliability. This means that the media server is duplicated, so that one is always active and the other is on standby — ready to take over in case the active one goes down. This duplex-reliability configuration is shown in Figure 13, S8700 IP Connect duplex reliability, on page 104.

# Basic server and IPSI connections

The S8700 Media Server uses the IP Server Interface (IPSI) to control port networks and provide tone, clock, and call classification services. The IPSI board connects to the control network by way of Ethernet.

---

### S8700 IP

The IPSIs provide transport of CCMS messages over IP allowing the media server to communicate with the port networks over the customer provided LAN. In an IP Connect configuration, there are two media servers and one IPSI per port network. Each media server is connected to the Ethernet switch which is on the LAN for connectivity to the IPSIs.

IPSI circuit packs are described in more detail in the *Hardware Guide for Avaya Communication Manager, 555-233-200*.

---

---

### S8700 MC

## High reliability connectivity

In a high-reliability Multi-Connect configuration there are duplex media servers, duplex control networks, and duplex IPSIs in each of the IPSI-connected port networks. However, the bearer network is not duplicated. The control network is duplicated so that a single fault in the control network, such as a bad Ethernet switch, will not bring the whole system down.

Each of the media servers connect to each of the control networks via the Ethernet switches. Each of the Ethernet switches connect to each of the IPSIs in the port networks. Each of the port networks connect to the single bearer network.

A port network can be IPSI-connected or non-IPSI-connected. In the high reliability configuration, all IPSI-connected port networks must have duplicated IPSIs. The non-IPSI-connected port networks will have nonduplicated Tone/Clock boards.

## Critical reliability connectivity

In a critical-reliability configuration there is full duplication of these components:

- Media servers
- Control networks
- IPSI circuit packs
- Bearer networks

The addition of duplicated bearer networks requires that each port network be connected to each bearer network. As with the high-reliability configuration, this configuration also requires that IPSI-connected port networks have duplex IPSIs. This configuration additionally requires that the non-IPSI-connected port networks have duplicated Tone/Clock boards (either TN2182 or TN780).

## Standard and High Reliability configurations

**S8700 IP**

In a duplex-reliability configuration, only the media server is duplicated; the IPSIs, control networks and bearer networks are not. Multiple Ethernet switches might be present in order to provide sufficient Ethernet connections to the IPSI circuit packs in the port network.

**Figure 13: S8700 IP Connect duplex reliability**

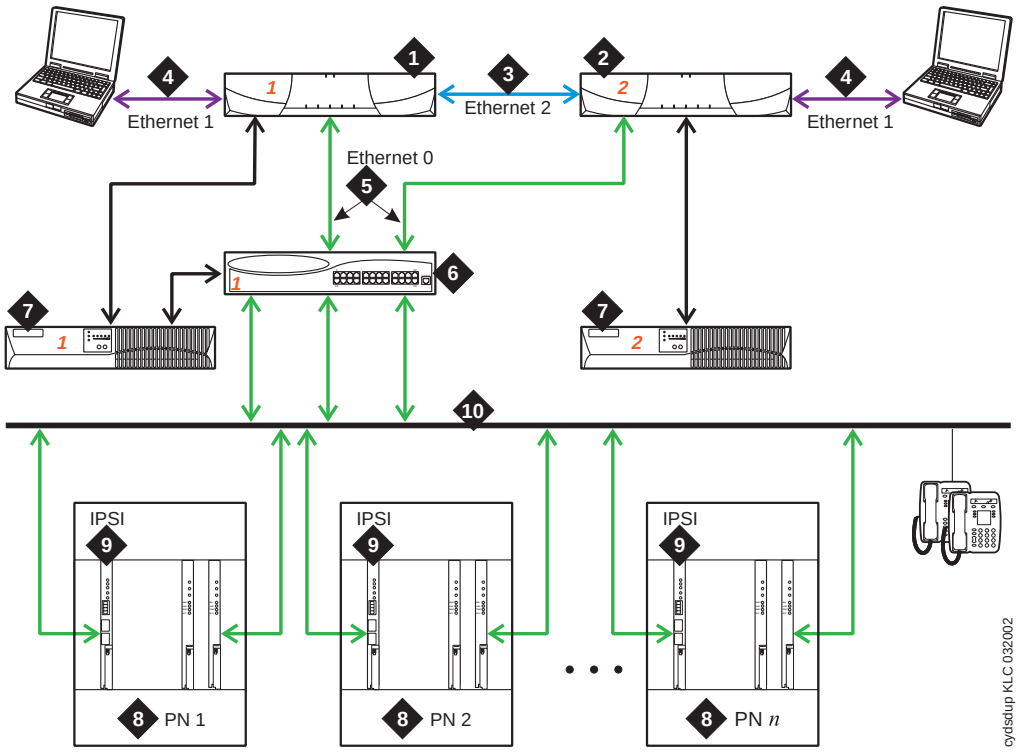



**Figure notes**

**1** S8700 Media Server 1

**2** S8700 Media Server 2

**3** Duplication interface – the Ethernet connection between the two S8700 media servers

**4** Services interface – dedicated Ethernet connection to a laptop. This link is active only during on-site administration or maintenance and the services interface can link to the non-active server through a Telnet session.

**5** Connection from the servers to the Ethernet switch.

**6** Ethernet switch – A device that provides for port multiplication by having more than one network segment. In an IP Connect environment, the Ethernet switch should support 802.1 IP/Q, VLAN, and 10/100 Mbps.

**7** Uninterruptible power supply (two required)

**8** Port network – optional configuration of media gateways that provides increased switch capacity

**9** IPSI – provides transport of CCMS messages over IP allowing the S8700 media server to communicate with the port networks.

**10** Customer LAN

**S8700 MC**

**Figure 14: High reliability for Multi-Connect configuration**

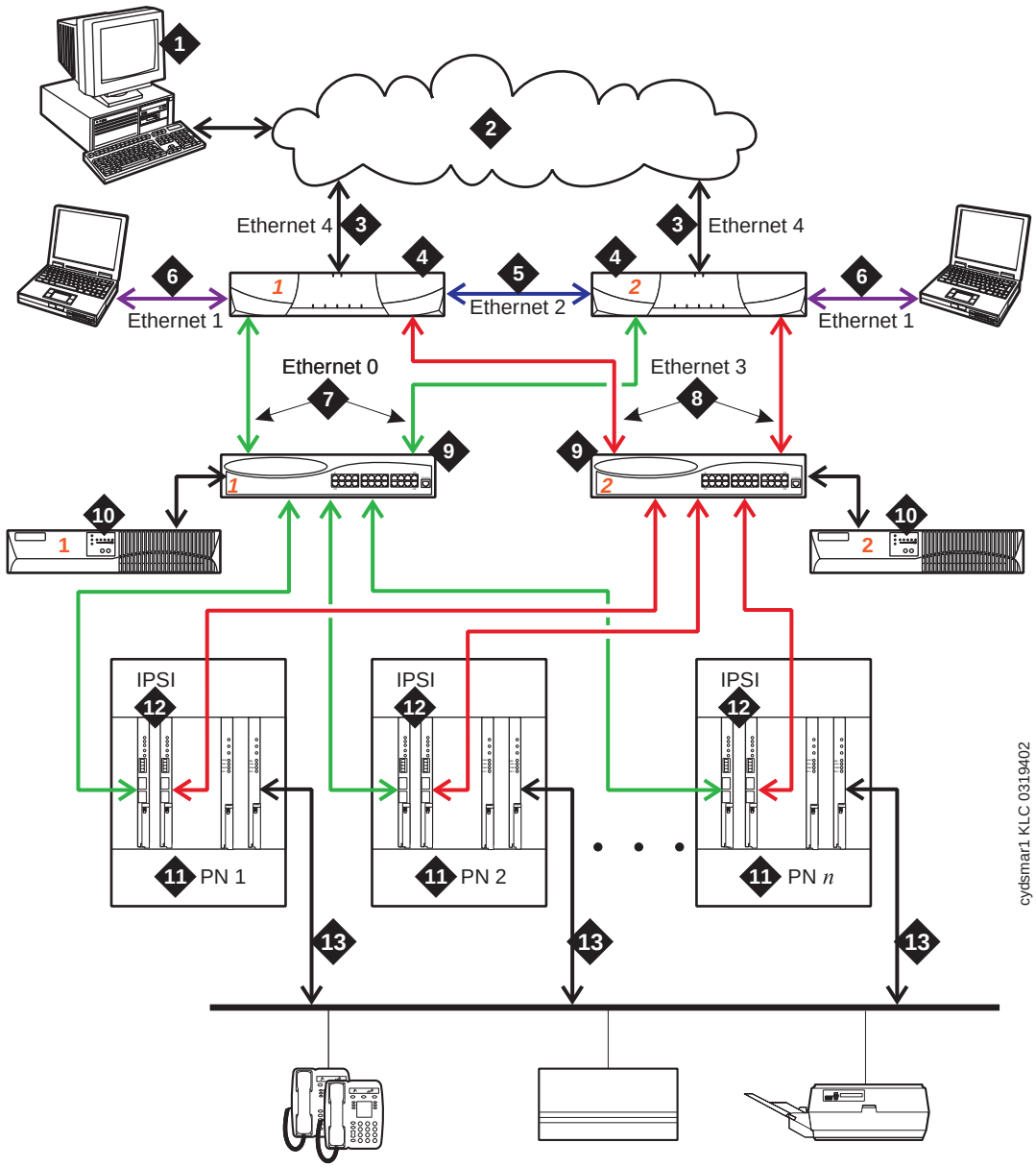


**Figure notes**

**1** Administration PC — used to access S8700 Media Server over the corporate LAN

**2** Corporate LAN

**3** Corporate LAN interface: default Ethernet 4 — S8700 Media Server's Ethernet link to the LAN. Used for administration and can be used for alarming through simple network message protocol (SNMP) traps to the Initialization and Administration System (INADS).

**4** S8700 Media Server — two are always present, one in active mode and the other on standby.

**5** Duplication interface: default Ethernet 2. The dedicated Ethernet connection between the S8700 Media Servers.

**8** Network control B interface: default Ethernet 3. The server's Ethernet connection to a duplicated set of Ethernet switches.

This private LAN carries control signals for the PNs when the primary control network is unavailable.

Control network B connects to the secondary IPSI board in a PN. When the system problem is resolved, primary control is returned to control network A.

**9** Ethernet switch — at least one is required to support each control network.

**10** UPS — Keeps the S8700 Media Servers and Ethernet switches functional through brief power outages. Usually, UPS 1 powers server 1 and its Ethernet switch, and UPS 2 powers server 2 and its Ethernet switch.

**11** PN — provides telecommunications functions of the S8700 Multi-Connect Media Server.

For High Reliability, each IPSI-connected PN contains a pair of IPSI circuit packs, one primary circuit pack and a duplicate secondary circuit pack as a backup.

For Critical Reliability, the bearer network among the port networks is also duplicated. This means that two EI circuit packs or two ATM circuit packs are present in each PN instead of just one.

**12** IPSI — IPSI circuit pack is duplicated in every IPSI-connected PN in a high reliability or critical reliability configuration.

The primary IPSI is connected to control network A. It is the preferred IPSI because it has better control over activating the clock than the secondary IPSI.

The secondary IPSI is connected to control network B. This IPSI takes over in case of problems with the primary control network. The S8700 Media Server regularly tests the duplicated IPSI to make sure it is ready for service, before returning control to the primary IPSI.

**Figure notes**

**6** Services interface: default Ethernet 1. The server's dedicated Ethernet connection to a laptop. This link is active only during on-site administration or maintenance.

**7** Network control A interface: default Ethernet 0. The server's Ethernet connection to 1 or 2 Ethernet switches. This private LAN carries the control signals for the S8700 Multi-Connect PNs when possible. Control network A is considered the primary control network because it connects to the primary IPSI board in a PN.

**13** Bearer network

## Critical Reliability configuration

Critical-reliability systems include all of the features and components of the high-reliability configuration described above, but it also has a duplicated bearer network. This configuration requires that not only the IPSI-connected port networks have duplicated IPSIs, but the non-IPSI-connected port networks must have duplicated Tone-Clock boards. Also duplicated in this configuration are the expansion interface (TN570) and the switch node interface (TN573).

# S8100 Media Server components and functionality

- TN2314 processor circuit pack on page 113
- Virtual boards and devices on page 108
- Windows 2000 platform on page 108
- GUI operation on page 109
- Backup procedures on page 109
- Access Security Gateway on page 111

## TN2314 Processor circuit pack

The TN2314 processor provides:

- An on-board Pentium III processor chip that runs Windows 2000
- A Motorola processor running application firmware
- A Windows 2000-to-firmware interface
- A tone clock

- A 1A11 virtual alarm board
- A 1A12 virtual INTUITY AUDIX board
- A 1A13 virtual announcements board

See the *Hardware Guide for Avaya Communication Manager, 555-233-200* for more information regarding the TN2314.

## Virtual boards and devices

The TN2314 processor circuit pack includes functions (such as the tone clock) that had previously resided on separate circuit packs. Commands, tests, and maintenance objects that were valid for the separate circuit packs are still available.

Virtual boards residing on the TN2314 processor circuit pack include:

- The 1A11 board used by Communication Manager to provide External Device Alarm contacts to indicate presence of any non-Communication Manager alarms. For more information see PR-AL-BD (Processor Alarm Board) in *Maintenance Alarms Reference (555-245-102)*.
- A virtual INTUITY AUDIX board (PR-SSP) resides in slot 1A12. The hardware for this board is located on the TN2314, but the INTUITY AUDIX ports on the board are administered as if they were physical ports on the virtual board. For more information see PR-SSP (Processor Board - Scalable Speech Processor).
- A virtual announcements board resides in slot 1A13. The hardware for this board is located on the TN2314, but the announcement ports on the board are administered as if they were physical ports on the virtual board. For more information see PR-SSP (Processor Board - Scalable Speech Processor).

## Windows 2000 platform

The TN2314 Processor circuit pack runs Microsoft Windows 2000. All applications run in the Windows 2000 environment.

> **NOTE:**
> If Windows 2000 is running on a laptop computer, set the terminal type to W2KTT for telnet sessions. For more information, refer to *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

Table 43, Applications installed on the S8100 Media Server, on page 109 lists the applications that are installed or available on the S8100 Media Server.

**Table 43: Applications installed on the S8100 Media Server**

| Application | Description |
|---|---|
| Communication Manager | Provides Communication Manager call processing features |
| INTUITY AUDIX | Provides voice mail |
| SNMP | Standard protocol for managing data network devices (Release 10 and higher) |
| Avaya Site Administration | Available for download |
| Message Manager | Available for download |
| BCMS Vu | Available for download (Release 10 and higher) |
| CentreVu T-Server | Available for download (Release 10 and higher) |

## GUI operation

The S8100 uses Avaya Site Administration, which has a graphical user interface (GUI) for all functions. See Chapter 2, "Connectivity and Access to S8100" in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

## Backup procedures

Since the system combines Communication Manager, INTUITY AUDIX and Windows 2000 on one platform, there is a new procedure to back up user information and translations.

Backup is performed in one of these ways:

- Using the web browser
- Using the UNIX-like bash shell, accessed via a Telnet session
- Using S8100, with a series of global administration system (GAS) commands (see Chapter 3, "S8100 Global Administration Subsystem Commands" in *Maintenance Commands Reference (555-245-101)* for a list of commands)

**NOTE:**
If a backup or restore operation is in progress, no other backup or restore command can be executed until the first one has finished.

**NOTE:**
Registry entries for IP addresses are not saved with the backup procedures. You must manually copy any registry entries that you want to save.

## How backup works

The S8100 system performs a backup by copying the files to be stored into a destination directory.

1. All files currently in the directory are removed prior to backup.
2. An identification file (ident file) is created for each backup, listing:
   - Version of backup program
   - Date and time the backup started
   - Date and time the backup completed
   - Code indicating successful completion or reason of failure
   - Indication of full or partial backup
3. A global alarm is raised if an error occurs during a backup operation.
4. Checksum verification is performed on all translation files.

**WARNING:**
Saving translations through the hard drive does *not* constitute a system backup. The data can still be lost.

A **save translation** command from Communication Manager saves translations data on the hard drive of the TN2314.

## Where to save translations and system user data

Once the data has been placed on the hard drive, it should also be saved on a backup drive. Data can be backed up to:

**Table 44: Storage locations for S8100 system user data**

| Location | Description |
|---|---|
| PCMCIA Flash Disk | The flash disk is a nonvolatile storage device installed in a PCMCIA slot on the TN2314.<br>A system backup to flash card will save ***only***<br>• Windows system registry<br>• Communication Manager translations<br>• INTUITY AUDIX translations (for small systems only)<br>• Header information for INTUITY AUDIX messages<br>**WARNING:**<br>Messages should ***not*** be saved on the flash disk, because there is limited space. If you want to save messages, you must back up the files to another device on the customer network. |
| Network device | You can back up all applications and messages to any network device that has enough storage, and is accessible across the network by S8100. Such devices include:<br>• Network disk drives<br>• Servers<br>• Tape drives<br>• Writable CDs |

## Access Security Gateway

Access Security Gateway (ASG), formerly SoftLock, is part of Avaya Site Administration. ASG is a centralized access interface that uses a challenge/response protocol to verify the authenticity of a user and to reduce the opportunity for unauthorized access. This is done through a key made of up to 20 octal digits.

**NOTE:**
ASG provides restricted access to Avaya Site Administration software. It does not access a switch.

This section provides information on how to administer and use Access Security Gateway Mobile (ASG Mobile). The procedures described here assume you have ASG Mobile installed on your PC.

ASG Mobile employs a challenge/response protocol to confirm the validity of a user and reduce the opportunity for unauthorized access. ASG authentication is imposed for Avaya Services logins as indicated below.

- lucent1 — all types of access require ASG authentication
- lucent2 — all types of access require ASG authentication
- lucent3 — all types of access require ASG authentication

**NOTE:**
init, inads, and craft are NOT supported on this platform — these logins are replaced by the lucent1, lucent2, and lucent3 logins.

### Using the ASG Mobile

1. On your desktop, double-click ASG Mobile V1.1.

   The ASG Mobile V1.1 window appears.

2. In the `Tech ID` field, type your login ID, which is the name of the attached file (without the.asg extension). Your login ID is the same as your Avaya login or an abbreviated part of it.

   **NOTE:**
   Your new password will be sent to you in a separate e-mail. The password is case-sensitive.

3. Type the password twice.
4. Click **OK**.

   The ASG Mobile V1.1 window appears.

5. Use your communications package (for example, ASA, ProComm, or TerraNova), to dial the switch you need to contact.
6. In the communications package window, login as **lucent1** or **lucent2**.

   Instead of a password prompt, a 7-digit challenge numbers appears.

   **NOTE:**
   Internationally, the correct logins are **lucent2** or **lucent3**.

7. Move to the ASG Mobile V1.1 window.
8. In the `Equipment ID` field, type the 10-digit Product ID.

   The default ID is 10 zeros (0000000000).

9. In the `Equipment Login` field, type **lucent1**, **lucent2** or **lucent3**.
10. In the `Challenge` field, type the 7-digit challenge number from Step 6. Do not use the "-" character.

    Communication Manager verifies the response. If correct, Communication Manager logs you on.

11. If the response is incorrect, return to Step 1.
12. If this is the third rejection, see the *Maintenance for Avaya DEFINITY® Server CSI* (555-233-119).

## G600 and CMC1 Media Gateways design

This section describes major design highlights for the G600 and CMC1 Media Gateway cabinets.

For further information, see the *Overview for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateway, 555-233-231*.

## TN2314 processor circuit pack

The TN2314 Processor circuit pack is the hardware component of the S8100 Media Server and is the heart of the G600 and CMC1 Media Gateway systems. It uses Microsoft Windows 2000 server as its operating system, allowing for graphical user interaction, network connections, standard applications, and coresidency and multitasking of applications. It is always found in slot 2 of either carrier type (see Figure 15, S8100 with the CMC1 slot configuration, on page 115 or Figure 16, G600 Media Gateway (IP600) slot configuration, on page 117).

The TN2314 features include:

- Dual processor complex consisting of an Intel Pentium III and Motorola processors
- 16 Mbytes of FLASH PROM for software text
- 256 Mbytes of SDRAM for translations and other data
- Supports up to 512 Mbytes of SDRAM
- 20 Gbyte hard disk drive
- RS232 port for the external modem

  The CMC1 and G600 Media Gateways use an external modem for alarm reporting to INADS and remote access. The approved modem is the U. S. Robotics Model 839 Sportster 33.6 Fax Modem (shipped with the CMC1 and G600 systems)
- Connectors for local devices (keyboard, mouse, and monitor)
- New “Services Ethernet” RJ-45 jack on faceplate (eliminates need for PCMCIA Ethernet LAN card)
- TN744B/C/D/E circuit pack functionality soon to be co-resident on the TN2314
  - Tone detection -- 8 ports on the TDM bus
  - Global Call Classification -- improved algorithms
  - Multi-Frequency (MF) signaling
  - Frees up a carrier slot

## Reliability options

The G600 and CMC1 Media Gateways do not support either high- or critical-reliability duplication or expansion options.

## AC power supply unit (650A)

The G600 and CMC1 Media Gateways use the same power supply unit, which contains:

- Multiple DC outputs: ± 5.1 VDC, -48 VDC, +8-14 VDC (fan speed control), and -150 to -115 VDC (Neon bus)
- Three switch-selectable AC ring outputs: 85 VAC @ 20 Hz (North America), 72 VAC @ 25 Hz (international), and two 28 VAC @ 50 Hz (France)

# CMC1 Media Gateway cabinets

A CMC1 Media Gateway configuration can contain three 10-slot Compact Modular Cabinets (CMC1) which include:

- Slots for circuit packs
- Power supply

## Slots

Each CMC1 has:

- Two shelves, each containing 5 slots
- Slots numbered 1-5 (lower shelf), and 6-10 (upper shelf)

  Three slots are reserved (2 slots for the processor and one slot for the tone detector circuit pack).

  **NOTE:**
  The TN2314 Processor circuit pack must be installed in slot 2 of the primary cabinet (due to width, slot 1 is unavailable).

  There are no restrictions on slot usage in the additional cabinet. Any slot can contain any type of circuit pack — port, control, or service.

For more information about slot configuration in the primary CMC1, see Figure 15, S8100 with the CMC1 slot configuration, on page 115.

**Figure 15: S8100 with the CMC1 slot configuration**

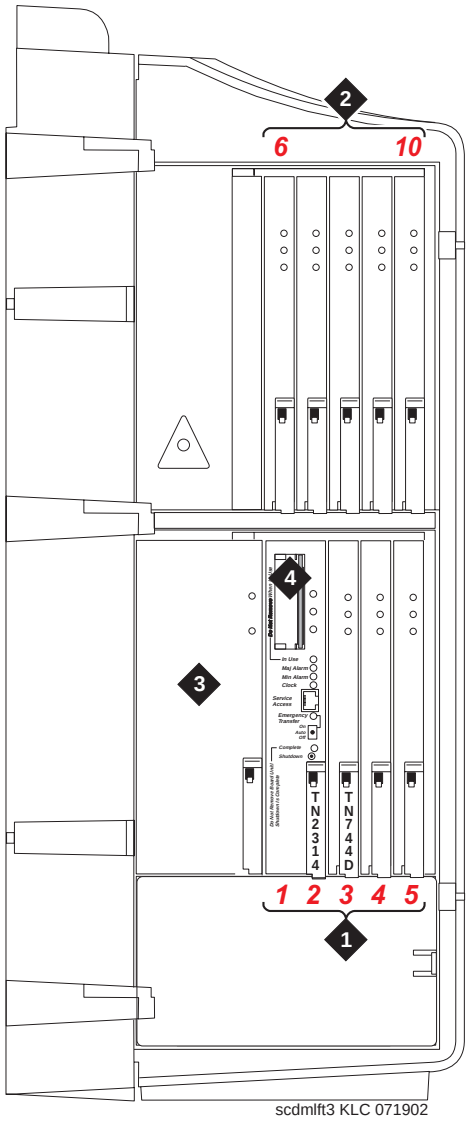



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Circuit pack slots 1 through 5 | **3** | Power supply |
| **2** | Circuit pack slots 6 through 10 | **4** | PCMCIA hard disk |

**WARNING:**
The TN2314 processor circuit pack must be placed in slot 2 (shown)

# G600 Media Gateway cabinet

A G600 configuration can contain two 10-slot rack- or shelf-mounted systems, which include:

- Slots for circuit packs
- Power supply

## Slots

Each G600 Media Gateway cabinet has:

- A shelf containing 10 slots, numbering 1-10

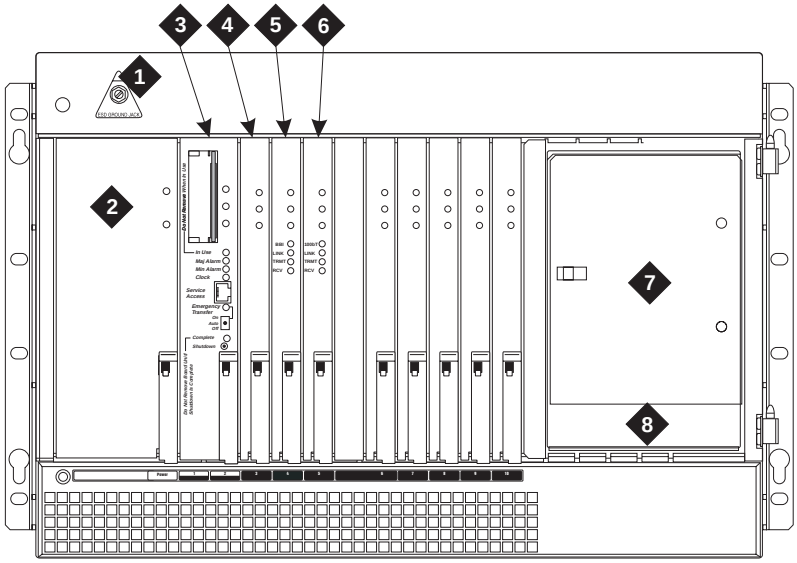
  Three slots are reserved (2 slots for the processor and one slot for the call classifier/tone detector circuit pack).

  **NOTE:**
  The TN2314 Processor circuit pack must be installed in slot 2 of the primary cabinet (due to width, slot 1 is unavailable).

  In the additional cabinet available in Release 2, there are no restrictions on slot usage. Any slot can contain any type of circuit pack — port, control, or service.

For more information about slot configuration in the primary G600, see Figure 16, G600 Media Gateway (IP600) slot configuration, on page 117.

**Figure 16: G600 Media Gateway (IP600) slot configuration**




scdpff02 KLC 071902

**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Grounding receptacle | **5** | TN799DP C-LAN |
| **2** | 650A Power Supply | **6** | TN2302AP IP Media Processor |
| **3** | TN2314 Processor | **7** | Storage (grounding wrist strap, backup PCMIA flashcard, and software and documentation library CDs, etc.) |
| **4** | TN744 Call Classifier-Detector | **8** | Fiber pass-through area |

## UPS

Use of an optional Uninterruptible power supply (UPS) between the AC power source and the switch is recommended to maintain service without interruptions.

- There is no battery backup available within the S8100 Media Server.
- If power is interrupted for more than 50 milliseconds, all calls are dropped and dynamic memory is lost.
- An external alarm is reserved for the UPS on the TN2314 processor circuit pack.
  - — If power is interrupted for more than one minute, a major alarm is raised.
  - — The TN2314 processor will attempt to shut the system down gracefully.

## Circuit packs

All circuit pack slots in the CMC1 and G600 Media Gateways are “universal slots.” That is, any slot can contain any type of circuit pack (port, control, or service), hence the absence of the purple and white slot coding found on other MultiVantage Applications products. The only requirements for slot allocation are:

- Service circuit packs are the only packs allowed in the CMC1 or G600. These “universal” service packs can be located in any slot numbered 3-10.
- A TN744D Call Classifier/Tone Detector circuit pack is required in S8100 server with the G600 or CMC1. This circuit pack can be installed into any slot, although slot 3 is preferred.

**WARNING:**

The TN2314 Processor circuit pack must be located in slot 2. Figure 16, G600 Media Gateway (IP600) slot configuration, on page 117 also shows the PCMCIA disk drive location.

# G700 with a Media Server system

The G700 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 G700 system is that it provides a standards-based, IP communications infrastructure that enables Avaya to lower customers’ total cost of ownership (i.e. applications to the edge of the network, high reliability for critical applications, and multi-service networking with feature transparency). The G700 with a Media Server infrastructure is comprised of three modular elements: Media Gateways, Media Servers, and Software.

## How does the G700 fit into your system?

The G700 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 is built on Cajun data equipment technology in order to integrate naturally into customer data networks and provide additional value in a Cajun networking environment. It provides the highly reliable Cajun hardware scheme with high-speed octaplane technology. See *Avaya P330 Manager User Guide* for more information on the Cajun hardware.

For introductory information about the S8300 Media Server or the G700 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*.

# 5 Server initialization, recovery, and resets

This chapter describes various maintenance aspects of media servers and their troubleshooting, including:



**S8700**

## S8700 Initialization

After a server is powered on, software/firmware modules are executed in the following order:

1. **BIOS** — The BIOS (Basic Input/Output System) takes control of the server's Pentium processor and provides several services including:
   - Running diagnostics on the server's hardware (processor, memory, disk, etc.).
   - Reading the 512-byte master boot record (MBR) from the boot sector of the boot disk into memory and passing control to it. The MBR contains phase 1 of the Linux loader (LILO).
2. **LILO** — The Linux loader (LILO) reads the Linux kernel from the boot disk and transfers control to it. Phase 1 of LILO was read into memory by the BIOS. When Phase 1 begins executing, it reads in the rest of the LILO program, including the Linux kernel's location. LILO reads in the Linux kernel, uncompresses it, and transfers control to it.
3. **Linux Kernel** — The Linux kernel initializes the Pentium processor's registers, initializes its own data structures, determines the amount of available memory, initializes the various compiled-in device drivers, etc. When finished, the Linux kernel creates the first process, known as *init*.
4. **Init** — The *init* process creates the remaining processes for the system using the `/etc/inittab` file, which specifies runlevels, and a set of processes to run at each runlevel.

   The rc script runs the service startup scripts in `/etc/rc.d/rc4.d` in numeric order (S00* through S99*). Each of these startup scripts starts a particular Linux service (e.g., inetd). In addition to starting up the various services, the disk partitions are checked for sanity, and loadable modules are loaded.
5. **Watchdog** — The Watchdog process (started by the rc script) reads its configuration file to determine operating parameters and applications to start up. Some of these applications include (in start-up order):
   - **a** Log Manager
   - **b** License Server
   - **c** Global Maintenance Manager (GMM)
   - **d** Arbiter

**e** DupMgr

**f** Avaya™ Communication Manager

These applications come up and start heartbeats to the Watchdog.

**NOTE:**
Use the Linux command **statapp** to view the status of the applications.

The Watchdog also starts up a script to monitor Linux services. It starts up threads to communicate with a Hardware-Sanity device.

**6** Hardware-Sanity — The Watchdog periodically tells the hardware-sanity device how long to wait before rebooting the system. If the Hardware-Sanity driver doesn't receive an update within that interval, the HW Watchdog's timer resets the processor.

**7** Arbiter — The Arbiter decides whether the server goes active or standby.

## Active server's initialization

These steps are executed on the server or active server (duplicated):

**1** Avaya™ Communication Manager — The Watchdog process creates the Communication Manager application by starting up the Process Manager (prc_mgr). The Process Manager starts up the Communication Manager processes by:

- Reading the Process Table file (`/opt/defty/bin/Proc_tab.z`)
- Creating every process with the PM_INIT attribute

Other Communication Manager processes (i.e., "initmap" and "hmm") create other "permanent" Communication Manager processes.

The Process Manager also:

- Verifies that Communication Manager is authorized to run on this server.
- Maintains a heartbeat to the Watchdog.

## Standby server's initialization

These steps are executed on the standby server:

**1** Avaya™ Communication Manager — On the standby server, many processes are frozen so that the Standby DupMgr can shadow into them without interfering with those writes. However, some shadowed and unshadowed processes need to run on the standby. These processes are known as the "run-on-standby" processes, and they have the RUN_STBY attribute.

The PCD process runs on the standby to communicate with port networks. The rest of these processes support the PCD or create processes that need to be shadowed into.

Some of the processes are:

- prc_mgr (Process Manager) — unshadowed
- phantom — unshadowed
- net_mgr — unshadowed
- tim — unshadowed

- tmr_mgr — unshadowed
- pcd — shadowed

  The active server's PCD shadows into the standby's PCD, so the standby's PCD does not to write to shadowed memory. The standby's PCD handshakes with every administered PN and counts accessible PNs to include in state-of-health reports to the Arbiter.

---

---

**S8100**

# S8100 Initialization

When the system is initially powered up, or when an existing system experiences a catastrophic fault that interrupts its basic functions, the system either initializes or reboots.

## LED boot sequence

### TN2314 processor circuit pack

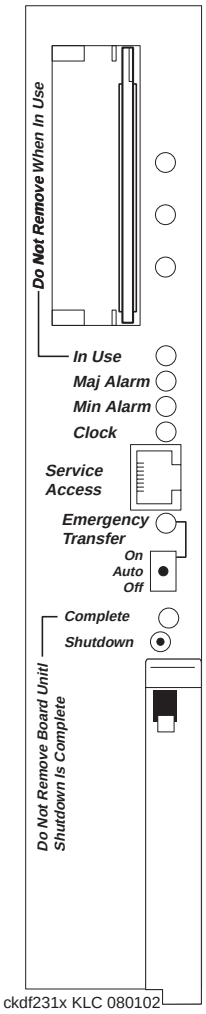
When power is first applied to the S8100, or when the system reboots, the LEDs on the TN2314 circuit pack will light according to this sequence:

1. All lights on the TN2314 will rapidly blink in sequence, from bottom to top (also known as "racing lights"). All lights will then be off.
2. Within one minute, the second light from the top will blink green:
   - When the LED is more on than off indicates BIOS loading
   - More off than on indicates Windows 2000 loading
3. The third LED from the top will blink amber to indicate application firmware loading.
4. When firmware is loaded, the LEDs will blink in sequence again (racing lights), then all LEDs will light and then go off.

   The S8100 system is now under normal operating conditions. When the system is operating normally you will see:
   - The amber LED (third from the top) will blink quickly once every 10 seconds, indicating the firmware/Windows 2000 watchdog processes are running.
   - The CLOCK LED will blink once every four seconds.

Any other LEDs that are illuminated indicate an alarm or problem with the S8100.

**Figure 17: TN2314 processor panel**




### Other circuit packs

You might see some LEDs on power up on the other circuit packs. Under normal operation, you should not see LEDs lit on the circuit packs, with the following exception: A solid green LED on any circuit pack indicates that diagnostic tests are in progress on that circuit pack.

## Communication Manager initialization

Upon initialization, no forms are available until the Offer Category is set. (The remote INADS channel is available.) To set the customer options, login as *Lucent 1* and do the following:

1 Enter **change system-parameters offer-options** (Lucent 1, 2, and 3 logins only) and the following form displays

```
change system-parameters offer-options                          Page   1 of   1

                                  OFFER OPTIONS

              Offer Category: A

              Activate Offer? y
```

### Field descriptions

| | |
|---|---|
| `Offer category` | Only Type **A** is allowed. |
| `Activate offer?` | Type **y** if the entry for `Offer category` is correct and press **Tab**.<br>Type **n** if there is an error in the `Offer category` field and press **Tab**. Re-enter the correct Offer Category. |

2 After these two fields are filled and you press **Enter**, the system displays a message in the History window.

3 Select the Submit option to submit the form.

4 Use the **save translations** command to make the changes permanent.

**CAUTION:**
To avoid potential loss of service, ensure that your system's translations are protected by saving them to the PCMCIA disk.

---

## Shutdown

System Reboot (reboot nice) is a complete system shutdown followed by an automatic reboot. Use after updating the system or changing system parameters. The entire system can be gracefully and manually shut down using the "`stop`" command with various arguments:

- `stop -r` — Graceful reboot: shuts down software, powers down system, reboots system.
- `stop -h` — Graceful halt: shuts down software, powers down system. Useful for server replacement.

The entire set of Watchdog applications can be shut down and restarted using Linux commands:

1 "`stop -ac`" — Shuts down Communication Manager and every individual application to the Watchdog

2 "`start -ac`" — Restarts every individual Watchdog application, including Communication Manager

**NOTE:**
Use the **-?** option with the **`start`** or **`stop`** Linux command for information about command syntax and usage.

**CAUTION:**
Follow normal escalation procedures **before** shutting down **either** an application or the entire system. Then, execute the shutdown only when advised by the appropriate tier's Services representative.

When the entire system is shut down via the `stop` command, the Watchdog executes the Linux "`shutdown -r 0`" command, which is the normal way to reboot Linux.

When Watchdog terminates an individual process, it sends a SIGTERM signal. Shutting down a single application involves sending a SIGTERM signal to the application's "leader" process. The application receiving the SIGTERM signal is responsible to gracefully shut itself down. If this shutdown fails, Watchdog sends a S IGKILL signal to abruptly kill the application.

For Communication Manager, the Process Manager sends a SIGTERM signal to its own "pamshut" thread. The pamshut thread checks whether any critical SAT commands, like **save translations**, are active. If so, the thread waits a few seconds and checks again. If no critical SAT commands are active, either initially or after a few seconds, the pamshut thread requests a reboot from the Process Manager.

**NOTE:**
**S8100**: System Shutdown (shutdown system) — complete system shutdown without an automatic reboot. Typically used for planned shutdown. See Appendix D for shutdown and restart actions and Appendix G for bash commands in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

# S8100 recovery

## Watchdog and applications

The Watchdog process (started by the rc script) reads its configuration file to determine operating parameters and applications to start up. The Watchdog monitors the sanity of the various applications it initially created. It does this using two mechanisms. The Watchdog receives:

- A SIGCHLD signal if any process it created dies
- Periodic heartbeat messages from those processes

If heartbeat messages go away for a certain time, as specified in the Watchdog's configuration file, the application is killed. When an application terminates, either unintentionally died or intentionally killed, the Watchdog runs an application-specific recovery script that:

- May try to kill every process in the application
- Checks for and corrects any resource problems
- Tries to recreate the application

The Watchdog tries to recreate the application a specified number of times. If unsuccessful after that number of tries within the specified retry interval, the Watchdog runs the application's "total failure" script.

For Communication Manager, the recovery script kills every Communication Manager process. Its total-failure script kills off the Communication Manager processes and causes a Linux reboot.

## Watchdog and Linux

The Watchdog monitors several Linux services/daemons. Since the Linux *init* process originally started these processes, Watchdog can not use the SIGCHLD signal to monitor these processes. Instead, Watchdog uses a thread to periodically check the validity of the process identifier for each monitored processes. If invalid, the Watchdog calls a Linux script to stop and then restart the particular service. The Linux services monitored by Watchdog are:

- **atd** – at daemon (runs programs at specific times)
- **crond** – cron daemon (runs programs periodically)
- **dbgserv** – provides debugging services
- **httpd** – Apache hypertext transfer protocol server (provides Web service)
- **inetd** – Internet server daemon (provides telnet/rlogin/etc. connectivity)
- **klogd** – Linux kernel log daemon (manages logging from Linux kernel/drivers)
- **prune** – monitors and cleans up partitions
- **syslogd** – Linux system log daemon (manages logging from Linux services and applications)
- **xntpd** – network time protocol daemon (manages clock synchronizations across the network)

## Watchdog's HiMonitor

The Watchdog's HiMonitor checks for run-away processes and terminates them. HiMonitor deals with an infinitely looping process that prevents lower-priority processes from running. More specifically, the high-priority HiMonitor process periodically looks for responses from the low-priority LoMonitor process. If present, HiMonitor resets Watchdog's timer. If not, HiMonitor issues and logs a top command to determine which processes are taking up CPU resources. HiMonitor then takes one of three recovery actions in this order:

1. If a process within Watchdog's or the Process Manager's Linux process group, is consuming too high a percentage (percentage set in `watchd.conf`) of CPU occupancy, HiMonitor kills the process.
2. If no process is using too high a percentage, but more than 100 instances of the same monitored process is running, HiMonitor reboots Linux.
3. Does nothing and waits for the system to recover on its own.

If LoMonitor does not respond to a preset threshold of HiMonitor checks, then, as a final recovery action, HiMonitor reboots Linux.

**CAUTION:**
Escalate to an Avaya engineer for guidance with this recovery, because it is potentially disruptive. A process can legitimately occupy abnormally high amounts of processor time due to server load, and killing it could make the server totally unavailable.

However, with an engineer's guidance, recovery can be disabled by setting the sampling-interval or occupancy-threshold values to **0**. More likely, the sampling-interval and CPU-occupancy thresholds need to be fine-tuned to values that do not cause erroneous recovery attempts.

**NOTE:**
The value of the sampling interval must be greater than or equal to **0**. If the sampling interval is set to **0**, the **top** command is not run and no recovery is performed.

The threshold CPU-occupancy percentage must be between **0** and **100**. If the threshold CPU-occupancy percentage is set to **0**, no recovery is performed but the **top** command's output is logged.

Setting the sampling interval and the threshold CPU-occupancy percentage to **0** may help achieve stability by obtaining useful data without disrupting the processes.

## Watchdog's hardware timer

The Watchdog's HiMonitor resets the timer on the hardware Watchdog circuitry via the Hardware-Sanity device driver. If the Watchdog is unable to reset the timer, the timer's value eventually decrements to 0, and the processor is reset.

## Hardware-Sanity device driver

The Hardware Sanity device driver (loadable module) is a modified Linux driver for the hardware Watchdog. A Sanity thread periodically writes to the Hardware Sanity driver, which resets the timer on the hardware Watchdog. If the Sanity thread does not write to the Hardware-Sanity driver, the:

- Driver does not reset the timer on the hardware Watchdog
- Timer expires
- Hardware Watchdog reboots Linux

The driver has three capabilities: set time-out interval to a configurable value, reset the timer to the time-out interval, and reboot Linux.

## Rolling reboots

There may be cases where recovering the system using a reboot does not correct the problem. If this occurs, the server continually reboots. This repeated rebooting increases the difficulty of diagnosing the problem. The Watchdog handles this with fixed "`MaxReboots`" and "`MaxRebootInterval`" parameters in the **watchd.conf** file. These fixed values are set to 3 reboots within 60 minutes. If it detects the software is rebooting too quickly, Watchdog logs a message to **syslog** and does not start Communication Manager software.

## Restarts

Restart is a traditional Avaya term for a system restart of less severity than a full recreation. Restarts are accomplished by retaining the memory state of certain processes.

The WatchDog process is not restartable, nor can it invoke restarts in Communication Manager. No Watchdog-started applications can restart. They are reloaded, as previously described. If the Watchdog itself dies, the parent Watchdog process restarts it. If the Watchdog dies 10 times in 2 minutes, *init* logs a message to Syslog for the GMM to process. GMM lowers the system's state of health (SOH), which causes a server interchange. Eventually, the hardware Watchdog resets the processor, because Watchdog is no longer resetting the hardware Watchdog.

## Communication Manager resets

- Single-Process Restart

  The system automatically perform single-process restarts and logs them in the ECS logger. Use the Linux command line and apply "`tail`" or "`grep`" to the log file to see occurrences of single-process restarts.
- Reset Level 1 (Warm Restart) on page 153
- Reset Level 2 (Cold-2 Restart) on page 154
- Reset Level 4 on page 155

When the system is powered up, or when it experiences a catastrophic fault that interrupts its basic functions, it undergoes a reboot. The system uses less severe resets to recover from other, less disrupting errors. The technician can initiate resets with a command.

**CAUTION:**
Communication Manager application resets can have wide-ranging disruptive effects. Unless you are familiar with resetting the system, follow normal escalation procedures before attempting a demand reset.

If a reset fails to recover normal system operation, the firmware that controls reset will escalate to the next higher level, up to reboot if necessary.

**NOTE:**
Hot restarts are not supported for S8700 servers. An on-demand, planned, or scheduled interchange results in a warm restart of the standby server if it is in a refreshed state, or a cold-2 restart if it is not refreshed.

Table 45, Communication Manager resets, on page 127 lists the components that are subject to or affected by interchanges, the maintenance object (MO) that the error is reported against, and a link to more information about the interchange.

**Table 45: Communication Manager resets**

| Component | Configuration | Link to more information |
|---|---|---|
| Communication Manager | All | • SYSTEM (System) in *Maintenance Alarms Reference (555-245-102)*<br>• display initcauses in *Maintenance Commands Reference (555-245-101)* |
| IPSI | In Port Network | • reset ipserver-interface in *Maintenance Commands Reference (555-245-101)* |

*(1 of 2)*

**Table 45: Communication Manager resets**

| Component | Configuration | Link to more information |
|---|---|---|
| | High Reliability<br>Critical Reliability | • IPSV-CTL (Ipserver Interface Control) in *Maintenance Alarms Reference (555-245-102)* |
| Port Networks | Standard Reliability<br>High Reliability | • reset ipserver-interface in *Maintenance Commands Reference (555-245-101)*<br>• EXP-INTF (Expansion Interface Circuit Pack) in *Maintenance Alarms Reference (555-245-102)*<br>• EXP-PN (Expansion Port Network) in *Maintenance Alarms Reference (555-245-102)* |
| | Critical Reliability | • PNC-DUP (PNC Duplication) in *Maintenance Alarms Reference (555-245-102)* |

*(2 of 2)*

**S8100**

# Recovery from fatal errors in the S8100

In the S8100 system, there are two types of fatal software failure modes:

- Software failure, resulting in the failure of Communication Manager and INTUITY AUDIX
- Operating system failure, resulting in the failure of Windows 2000 (SPE-Down Mode)

Hardware failures can also be a root cause of fatal software failures. Hardware failures may also be accompanied by an illuminated red LED on the failing circuit pack.

## Firmware failure

The firmware automatically reboots the S8100 system when the handshaking signal between the firmware and Windows 2000 is not detected. If there are greater than 5 reboots in a 60-minute time period, the system is not self-repairing, and the firmware stops attempting to reboot Windows 2000.

### *To view the handshaking signal*

1. Observe the amber LED on the TN2314 processor circuit pack.
2. If it flashes briefly once every 10 seconds, the handshaking signal is present.

### *If there is no handshaking signal*

If the firmware has stopped, and Windows 2000 is running, you can use Windows 2000 to provide information to higher-tier personnel for troubleshooting.

### SPE-down mode

In the S8100 system, SPE-Down mode refers to the condition in which:

- Windows 2000 failed
- System firmware still running

The firmware will issue an INADS alarm call at 7 minute intervals. If the problem has not been corrected after the first three messages have been issued, the alarm call interval is increased to 45 minutes.

### Recovery from fatal errors

In general, if there is a fatal error, the system will not be operating at a level that can be investigated in the field.

If the S8100 has a fatal error:

1. Reboot the system. If you cannot access the system using any of the software methods, you can reboot the system by pressing the reset button on the TN2314 processor circuit pack.
2. Verify that you have no alarm leads on the TN2314 that could be shorted together to cause an SPE download.
   a. Check to see if UPS is being used.
   b. If yes, proceed to the next step.
   c. Check to see whether pins 26 and 1 are being used as other alarm inputs. Pins 26 and 1 on the AUX connector are dedicated to the UPS alarm input.
   d. If yes, disconnect from the other connections.
3. If the problem persists after reboot, you may have to replace the processor circuit pack.

## Resolving alarms

An alarm is generated when a non-fatal error is detected by the S8100 system. This section describes methods to determine the source of alarms.

### Recovery procedures

The first step is to determine the location of the problem. It is possible for two or more circuit packs to have failed. It is also possible for a fatal problem with one circuit pack to affect another circuit pack, especially the Processor circuit pack. To determine where the fatal fault lies, employ all three of the following methods:

- Using the bash shell in a telnet session on page 130
- Obtaining information from Communication Manager alarms on page 130
- Removing a system from the SPE-Down mode on page 130

### *Using the bash shell in a telnet session*

The bash shell opened during a telnet session is used to access the global platform level in the S8100 system. Once this interface is established:

1. Use **alarmstat** command.

   **alarmstat** will display all active global, Communication Manager and INTUITY AUDIX alarms.

2. If there are any global alarms, use **gamalarmstat** to see details of global alarms.

3. Use **restartcause** to obtain information about system restarts. See restartcause in *Maintenance Commands Reference (555-245-101)*.

For more information, refer to the manual *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

### *Obtaining information from Communication Manager alarms*

You can use the following Communication Manager commands to obtain more alarm information.

1. Use **display alarms** command:

   Issuing the **display alarms** command at the administration terminal shows where maintenance thinks the problem lies. The alarms are a good indication of why the system went down. They should be used along with the following two methods.

2. Observe red LEDs on the circuit pack to determine where software or processor firmware had a problem.

3. Use the **reset** command:

### *Removing a system from the SPE-Down mode*

> **NOTE:**
> **This is important!** If you cannot complete the first step or have problems with the maintenance interface, then the first step should be to replace the Processor circuit pack.

1. Determine which circuit pack is defective by displaying alarms and observing the red LEDs (as discussed previously).

---

# Link Recovery

Communication Manager offers two levels of Link Recovery:

- H.248 server-to-gateway Link Recovery on page 131
- H.323 gateway-to-endpoint Link Recovery on page 139

# 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

H.248 Link Recovery is compatible with:

- Avaya Communication Manager Release 1.3 and higher
- Avaya S8300/S8500/S8700 Media Servers with Avaya G700 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

## H.248 Link Recovery processes

This section describes the H.248 Link Recovery scenarios and the concurrent call handling and maintenance activities:



### *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 46, H.248 Link Recovery timers, on page 132 lists the timer parameters.

**Table 46: H.248 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 47, General Link Recovery process, on page 133.

**Table 47: General Link Recovery process**

| Process sequence | Description |
|---|---|
| 1. | Link failure detected (see Conditions that trigger Link Recovery on page 131) |
| 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.<br>See Administering the MGC list on page 137 for instructions on administering this list.<br>See Administering the gateway timers and Transition Point on page 136 for instructions on administering the Primary and Total Search Timers. |
| 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:<br>**S8300**: 1-3 S8300s configured as Local Spare Processors (LSPs)<br>**S8500 and S8700**: 1-3 C-LAN circuit packs within the primary server's configuration<br>The Total Search Timer continues running.<br>See Administering the MGC list on page 137 for instructions on administering this list and on 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 1 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 134 for more information about the server and gateway alarm notification strategies.<br>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 have been exhausted.<br>**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. |

### *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 ACD group, attendant group, call park, or are 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 137 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

### *Server alarms*

Expiration of the Link Loss Delay Timer triggers Communication Manager alarm notification. These events and their associated alarm levels are in Table 48, Avaya Communication Manager alarms, on page 134.

**Table 48: 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 49, Media Gateway events and alarms, on page 135.

**Table 49: 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. Use these links to go to the appropriate section:


- Administering the server timer on page 135
- Administering the Media Gateway on page 136
  - Administering the gateway timers and Transition Point on page 136
  - Administering the MGC list on page 137


### *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, which drops all calls in progress.

#### *To administer the Link Loss Delay Timer:*

1. At the SAT type **change system-parameters ip-options** and press Enter to display the system parameters ip-options form (Figure 18, System-parameters ip-options form, on page 136).

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 136).

3 Press Enter to save the change.

**Figure 18: System-parameters ip-options form**

```
display system-parameters ip-options

                      IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS
   Roundtrip Propagation Delay (ms)    High: 30       Low: 20
                   Packet Loss (%)     High: 10       Low: 5
                   Ping Test Interval (sec): 10
   Number of Pings Per Measurement Interval: 10

RTCP MONITOR SERVER
                  Default Server IP Address: 192.168.1  .12
                        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
            Link Loss Delay Timer (Minutes): 5
```

### *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 mgp 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 Administer the **Total Search Timer** (the length of time that the gateway spends trying to connect to all alternate resources) by typing **set mgp 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.

3 Establish the **Transition Point** by typing **set mgp reset 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 H.248 Link Recovery timers on page 132 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 4 elements in this list.

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

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**.

Look in the CONFIGURED MGC HOST section 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 50, H.248 Link Recovery feature/adjunct interactions, on page 138).

**Table 50: H.248 Link Recovery feature/adjunct interactions**

| 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. |
| 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.<br>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. |

## Network fragmentation

A likely outcome to an H.248 link recovery scenario is that a network of G700 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:

- Execute **reset system 4** on each LSP
- Shut down Communication Manager on every LSP

### *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 G700 containing an LSP, thus forcing any G700s 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 G700s 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** issued to each LSP will then restart Communication Manager on each of those platforms.

## H.323 gateway-to-endpoint Link Recovery

The H.323 link between an Avaya Media Gateway and an H.323-compliant IP endpoint 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 endpoint cannot reconnect to the original Gateway, then H.323 Link Recovery automatically attempts to connect with alternate TN799DP (C-LAN) circuit packs within the original server's configuration or to a Local Spare Processor (LSP).

H.323 Link Recovery does not diagnose or repair the network failure that caused the link outage, however it:

- Attempts to overcome any network or hardware failure by re-registering the IP Endpoint with its original Gateway.
- Maintains calls in progress during the re-registration attempt.
- Continues trying to reconnect if the call ends and the IP Endpoint has not yet reconnected to its original Gateway.
- Attempts connecting to and registering with an alternate Gateway if so configured.

Table 51, Synopsis of recovery outcomes, on page 140 provides a synopsis of the recovery outcomes.

**Table 51: Synopsis of recovery outcomes**

| If | Then |
|---|---|
| No Gateway is found | The endpoint is out-of-service until it can find a Gateway. |
| The IP endpoint registers with a new Gateway | The call ends and the endpoint is available (full features and buttons) through the new Gateway. |
| Original Gateway accepts re-registration | The endpoint is available (full features and buttons) through the new Gateway. |
| Call in progress but endpoint cannot re-register | A call in progress remains so.<br>No new calls are accepted.<br>Features and buttons are inoperable. |

## Software compatibility

The H.323 Link Bounce Recovery feature works when

- The Avaya Media Server is running Communication Manager Release 2.0 (and later)
- The IP endpoint firmware supports the feature (see IP endpoints supported).

If either one or both do not support the feature, then the IP Endpoint takes no action for the H.323 Link Bounce messages coming from the server.

## Hardware

This is a software feature that does not require the addition or presence of any hardware beyond that normally required for the support of IP Telephony is supported on the following platforms:

- DEFINITY series
- S8100
- S8300
- S8700

### *IP endpoints supported*

All IP endpoints can, but are not required to, support this feature. This includes softphones, IP telephones, and Avaya MVCS. As an example, a sampling of Avaya endpoints are listed below:

- Avaya IP Softphone; R5 for Windows 2000
- Avaya IP Softphone for Pocket PC
- Avaya IP Agent R5: firmware version 5.000 or above
- Avaya IP Agent R4

- MultiVantage Connection Server (MVCS) Version 2.0 and above
- Avaya Softconsole R2: firmware version 2.000 and above

> **NOTE:**
> As of this writing, there are no plans for the R2 version of Softconsole. But by the time it becomes available, the iClarity component that actually provides this feature will be available and that is what Softconsole will use.

## Interactions

### *Internationalization*

The H.323 Link Bounce Recovery feature does not rely upon nor is it affected by international telecommunications PTT variations or standards implementations.

### *Feature limitations*

Since there is no communication possible between the Gateway and the IP endpoint during a link outage, button depressions are not recognized, feature access codes do not work, and any other type of call handling ceases. In essence, the server cannot react to any stimuli until the H.323 signaling link is restored.

At a minimum, the features listed below might be impacted by a link bounce:

- Call Forward
- Call-coverage: stations
- Call-coverage: VDNs
- Call-pickup
- Displays
- Drop
- Group Page
- Hold
- IP-Direct/Shuffling
- Last Number Dialed
- Priority Calling
- Station Hunting
- Terminating Extension Groups
- Transfer
- TTI/PSA

### *Cross-Product compatibility/commonality*

In general, the time delay caused by a failed network connection could result in unacceptable outcomes, even though calls in progress are not lost. Although the IP endpoint might eventually reconnect to the original Gateway, the end user might experience what they perceive to be a lack of service while the endpoint is trying to re-register. Since users cannot put a call on hold, transfer, send-all-calls, and use other trivial or even advanced switch features, they might conclude that “the phones aren't working.”

Table 52, Cross-product interactions due to link failure, on page 142 describes the performance interactions due to link failure-induced time delays.

**Table 52: Cross-product interactions due to link failure**

| Product or adjunct | Description |
|---|---|
| Terminals | Time-of-Day, busy lamp states, and call appearance status on some sets might not instantaneously reflect the correct information until the H.323 Link Bounce Recovery process has successfully recovered the signalling link and synchronization has occurred. |
| Adjunct Switch Applications Interface (ASAI) | ASAI-based applications that utilize timing loops, time-related methods or events, might not accurately perform as intended. Furthermore, applications that depend upon a rigid state machine model and do not accommodate time-outs or missing state transition(s) might behave in an unpredictable manner. |
| Voice Mail adjuncts (AUDIX, Intuity, Octel) | During the recovery interval callers connected to AUDIX remain connected even if they hang up. AUDIX might automatically disconnect these calls if the connection remains intact without the calling party entering tone commands to AUDIX or voicing a message. AUDIX does not respond to button depressions during the link outage. |
| Call Detail Recording (CDR) | As a result of a link recovery, it is possible that the CDR 'call connection time' could be erroneous. |
| Call Management System (CMS) | Statistics might not accurately reflect actual usage; accuracy depends on the length of the outage. |
| Property Management System (PMS) | Time-related features such as Automatic Wake-up, Daily Wake-up, and Housekeeping Status do not operate at all or as expected if the H.323 link fails in the course of their activation. For example, wake-up calls might not ever occur if the link outage occurs at the time of the call. |
| Voice Response Systems (Conversant) | Conversant applications might not gracefully accommodate the loss of signaling to an endpoint to which the application is attempting to connect. |

### *Memory impact of capacity changes*

This feature does not impose any significant impact on memory beyond that normally required for call processing.

### *Performance impacts*

**Endpoint State Information Audit** Following the link restoration, the audit that is performed to synchronize endpoint state information between the server and the IP endpoint presents no more of a load than that required to perform the routine lamp and switchhook audit. However, if a large number of H.323 endpoints must re-register, server performance is likely to degrade during the re-registration process.

**Features and services** The H.323 Link Bounce Recovery feature impacts call processing only while the link is actually “down.” If a call on an IP endpoint is in progress when the link loss occurs, the voice-path on that call remains in service. However, access to and/or operation of any server-based features or services will not occur until the link is re-established.

During the recovery process, when the IP endpoint is attempting to re-register, the customer will experience some noticeable anomalies in the handling of some features or capabilities:

- An IP endpoints will not have dial-tone for a new call.
- Music or announcement sources connected to a call that includes an IP endpoint that has lost its signaling connection to the Gateway will remain in the context even if all parties to the call hang up.
- AUDIX connections timeout after the IP endpoint caller has left a message and hung up.
- If the outage persists for several minutes, the statistics for BCMS, CMS, call attendants, and other time-related reports might be inaccurate.
- If the endpoint hung up during the link recovery process, SMDR records will be inaccurate for the link recovery time period.
- The following IP Telephone buttons do not work:
  - TouchTone pad
  - Feature access buttons (Hold, Conference, etc.)
  - Administrable buttons
- The server maintains call state information for the IP endpoint for the duration of the H.323 Link Loss Delay Timer plus 15 minutes. At that time Communication Manager deletes the IP endpoint's call state, so that when the call ends, the IP endpoint must re-register. If the endpoint is operating in 'telecommuter' mode, this timer does not apply.

## Keep-Alive signals

IP Endpoints transmit either RAS Keep-Alive (the default) or TCP Keep-Alive signals. Through the use of Gateway-to-IP endpoint messaging, the IP endpoint transmits a compatible Keep-Alive message as instructed by the Gateway.

The RAS Keep-Alive signal frequency increases with an ever-increasing number of registered IP endpoints. To reduce the volume of the Keep-Alive messages on a server, Communication Manager varies the RAS time-to-live (TTL) value based on the number of registered IP endpoints and the server platform (DEFINITY series, S8700, S8500, S8300, and S8100). However, continually increasing the TTL to accommodate more IP endpoints eventually reaches a point where the time to detect and recover from a temporary signaling loss between the server (Gateway) and endpoint is unacceptable. For this reason both the endpoint and the Gateway (Communication Manager server) use TCP Keep-Alive messages to status the call signaling channel.

Communication Manager monitors a low-frequency TCP Keep-Alive signal from the Gateway to an endpoint to detect whether the endpoint is still accessible. This Keep-Alive allows the Gateway to detect call signaling channel failures in cases where the IP endpoint may have migrated to an LSP or has simply failed. If the IP endpoint is accessible, then it sends a TCP Keep-Alive signal to its Gateway (server) whenever the TCP connection is idle.

The TCP Keep-Alive mechanism for an endpoint depends on the:

- Idle Traffic Interval (see Figure 19, Idle Traffic Interval, on page 144)
- TCP Keep-Alive Interval (see Figure 20, Keep-Alive signals acknowledged by Gateway, on page 144)
- Keep-Alive Count (see Figure 21, Keep-Alive signals not acknowledged by Gateway, on page 145)

These three (3) administrable parameters are explained in Table 53, Administrable H.323 Link Bounce Recovery parameters, on page 145.

The Idle Traffic Interval is the period of time between the IP endpoint's last broadcast Keep-Alive signal and the Gateway's last acknowledgement as depicted in Figure 19, Idle Traffic Interval, on page 144.

**Figure 19: Idle Traffic Interval**

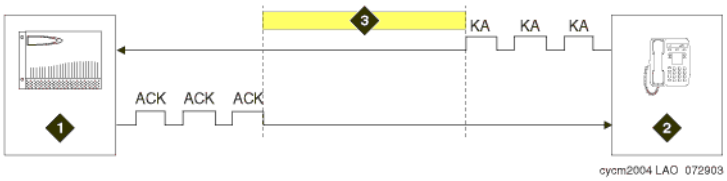



**Figure notes**

KA is the Keep-Alive signal; ACK is the Gateway's acknowledgement

| | | | |
|---|---|---|---|
| **1** | Gateway | **3** | Idle Traffic Interval |
| **2** | IP endpoint | | |

The Keep Alive Interval is the time between Keep-Alive messages that the endpoint sends to the Gateway as depicted in Figure 20, Keep-Alive signals acknowledged by Gateway, on page 144.

**Figure 20: Keep-Alive signals acknowledged by Gateway**

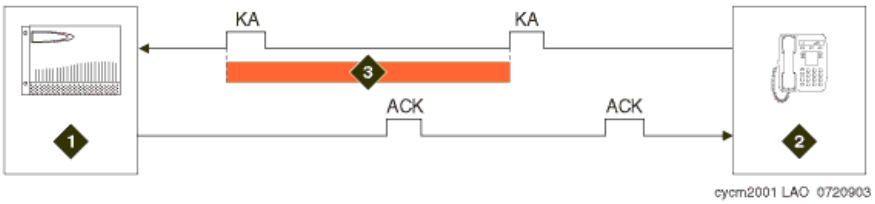



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Gateway | **3** | Keep-Alive Interval |
| **2** | IP endpoint | | |

Whenever the Gateway does not send the acknowledge message (ACK) in response to the endpoint's TCP Keep-Alive signal (KA), the Keep-Alive Count (note 4 in Figure 21, Keep-Alive signals not acknowledged by Gateway, on page 145) begins. After the administered number of Keep-Alive signals is reached (2 in the example), the endpoint attempts to re-register with the Gateway (note 5 in Figure 21, Keep-Alive signals not acknowledged by Gateway, on page 145).

The loss of the H.323 signaling link between the Gateway and an IP endpoint is detected by the TCP-based Keep-Alive signaling, and both the endpoint and the Gateway must be administered for the H.323 Link Bounce Recovery feature (see Administration).

**Figure 21: Keep-Alive signals not acknowledged by Gateway**

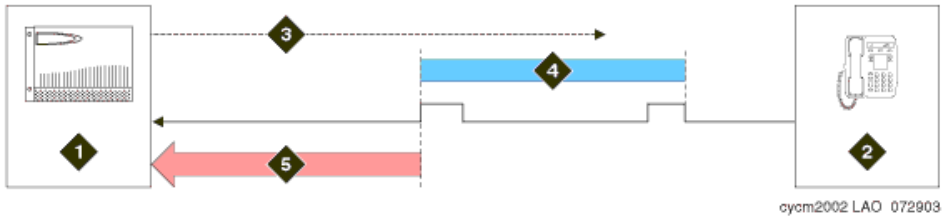



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Gateway | **4** | Keep-Alive Count = 2 |
| **2** | IP endpoint | **5** | Endpoint attempts to re-register with Gateway |
| **3** | No Gateway acknowledgement or H.323 link to IP endpoint | | |

Table 53, Administrable H.323 Link Bounce Recovery parameters, on page 145 lists the administrable parameters that interact within the H.323 Link Bounce Recovery feature. See Administration for how to implement these parameters.

**Table 53: Administrable H.323 Link Bounce Recovery parameters**

| Parameter (device) | Definition |
|---|---|
| Idle Traffic Interval (Endpoint) | The maximum traffic idle time after which a TCP Keep-Alive (KA) signal is sent from the endpoint. |
| Keep Alive Interval (Endpoint) | The time interval between TCP Keep-Alive re-transmissions. When no ACK is received for all retry attempts, the local TCP stack ends the TCP session and the associated socket is closed. |
| Keep-Alive Count (Endpoint) | The number of times the Keep-Alive message is transmitted if no ACK is received from the peer. |
| H.323 Link Loss Delay Timer (Gateway) | This timer specifies how long the Communications Manager server (Gateway) preserves registration and any stable calls that may exist on the endpoint after it has lost the call signaling channel to the endpoint. If the endpoint does not re-establish connection within this period, Communication Manager tears down the registration and calls (if any) of the endpoint.<br>**NOTE:**<br>This timer does not apply to Soft-endpoint telecommuter calls. |

*(1 of 2)*

**Table 53: Administrable H.323 Link Bounce Recovery parameters**

| Parameter (device) | Definition |
|---|---|
| Primary Search Time (GST) (Endpoint) | While on-hook, this is the maximum time period that the IP endpoint expends attempting to register with its current Communication Manager server (Gateway). The need for this timer arises in situations where the current Communication Manager server may have a large number of C-LAN circuit packs. This timer allows the customer to specify the maximum time that an IP endpoint spends on trying to connect to the C-LANs associated with the current Gateway before going to an LSP as defined in the Alternate Gateway List.<br><br>While off-hook, the endpoint continues trying to re-establish connection with the current server (Gateway) until the call ends. |

*(2 of 2)*

## Link recovery sequence

Table 54, H.323 Link Recovery sequence, on page 146 lists the sequence of events during recovery and includes an explanation of what it happening. This sequence correlates with Figure 22, H.323 Link Bounce recovery process, on page 148.

**NOTE:**
The sequence assumes that the Idle Traffic Interval and the Keep-Alive Interval are already administered at acceptable levels for the network configuration.

**Table 54: H.323 Link Recovery sequence**

| Process sequence | Description |
|---|---|
| **1** | Link failure detected (any of the following):<br>• Gateway detects a TCP socket failure<br>• TCP socket closure<br>• Catastrophic network error on the link<br>• Lack of a TCP Keep-Alive signal from the endpoint (Keep-Alive Count exceeded). See Keep-Alive signals and Note 4 in Figure 21, Keep-Alive signals not acknowledged by Gateway, on page 145 for more information. |

*(1 of 2)*

**Table 54: H.323 Link Recovery sequence**

| Process sequence | Description |
|---|---|
| **2** | The TCP Keep-Alive timer on the C-LAN circuit pack starts (15 minutes). If the signalling link is still down, the H.323 Link Loss Delay Timer begins (Note 2 in Figure 22, H.323 Link Bounce recovery process, on page 148).<br>• If the endpoint is on a call when the failure is detected, it tries to re-register with the address(es) of the same Gateway that it was registered with prior to the failure. The endpoint does not wait for the call to be over to re-establish the signaling channels. However, the endpoint does not try to connect to an address of a different Gateway while recovering from a failure encountered during an active call. This is because registering with another Gateway would result in call termination.<br>• If the endpoint is not on a call when the link failure is detected, the endpoint tries to connect to the address(es) of its primary Gateway. If the connection cannot be established with an address of the primary Gateway, the endpoint "marks" the Gateway as "unavailable" and tries to register with the address(es) of the next Gateway in the Alternate Gateway List. If all Gateways are marked, the endpoint stops the registration, "unmarks" all of the Gateway addresses in its list, and then displays an error message to the user.<br>**NOTE:**<br>During the re-registration process when an endpoint is on an active call, both the Communication Manager server and the endpoint take care that any existing calls are not dropped. In fact, if the re-registration completes successfully, the endpoint regains all call features. |
| **3** | If the endpoint is successful in connecting to the same Gateway, it re-registers, performing what amounts to as a "full" H.323 registration. An internal audit updates the lamp, button, and switchhook information and continues or closes SMDR according to the endpoint state. The Gateway recognizes the endpoint's identity as having previously registered and does not terminate the active call. |
| **4** | As soon as the endpoint detects that the user has hung up, it tries to connect to the address(es) of its primary Gateway if the Gateway Primary Search Timer (Figure 22, H.323 Link Bounce recovery process, on page 148) has not expired yet. |
| **5** | If the connection cannot be established with an address(es) of the primary Gateway or if the Primary Search Time (Note 3 in Figure 22, H.323 Link Bounce recovery process, on page 148) has expired, the endpoint then tries to register with the address(es) of the next Gateway in the Alternate Gateway List, as depicted by Note 8 in Figure 22, H.323 Link Bounce recovery process, on page 148). |
| **6** | The endpoint continues its re-registration attempts, as depicted by Note 9 in Figure 22, H.323 Link Bounce recovery process, on page 148. |
| **7** | When the H.323 Link Loss Delay Timer expires (Note 10 in Figure 22, H.323 Link Bounce recovery process, on page 148), the Gateway drops all call state information. |

*(2 of 2)*

Use Figure 22, H.323 Link Bounce recovery process, on page 148 below to correlate the events in Table 54, H.323 Link Recovery sequence, on page 146.

**Figure 22: H.323 Link Bounce recovery process**

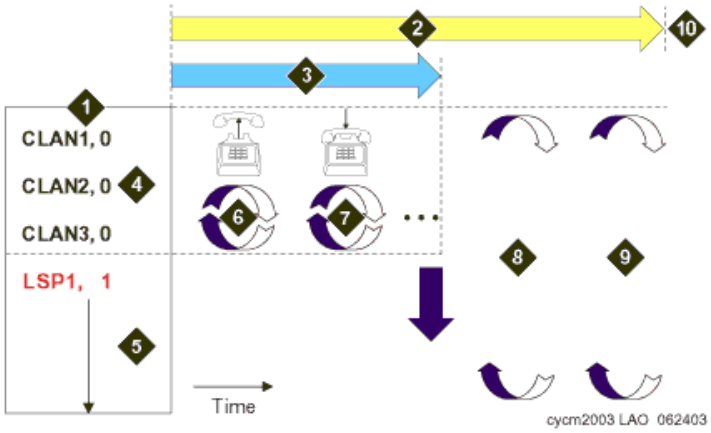



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Alternate Gateway List | **6** | Endpoint attempts re-registration while call is in progress |
| **2** | H.323 Link Loss Delay Timer (gateway) | **7** | Call ends and endpoint continues re-registration attempts |
| **3** | Primary Search Time (endpoint) | **8** | Endpoint attempts re-registration to any Gateway in the AGL, including Local Survivable Processors (LSPs) |
| **4** | IP address of alternate C-LAN and Gateway ID | **9** | Endpoint continues re-registration attempts. |
| **5** | Local Survivable Processor (LSP) list in search order. | **10** | Gateway deletes IP Endpoint's call state information when H.323 Link Loss Delay Timer expires. |

### *Alternate Gateway List*

The Alternate Gateway List (AGL) is created using an entry from DHCP, a TFTP script, DNS server, or manually by administration on the IP endpoint. It can contain the IP addresses of up to thirty (30) eligible Gateways that the IP endpoint can register with. In addition, there are three (3) parameters associated with the use of the Alternate Gateway List.

AGL changes made within Communication Manager administration are downloaded to the IP endpoint during the registration process and as soon as possible after any administration is performed.

Figure 22, H.323 Link Bounce recovery process, on page 148 depicts a network in which the Alternate Gateway List (AGL) has four (4) entries. Each entry includes an IP address of a C-LAN or an LSP, followed by a Gateway ID. The purpose of the ID is to differentiate the C-LAN addresses from an LSP address. For simplicity sake, the IP address is not shown in the figure. Instead the label 'CLANx' or 'LSPx' is used.

The three (3) C-LAN entries imply that the IP endpoint has three (3) different interfaces to the Communication Manager server that is hosting the Gateway function. Thus, for the purposes of registration to the Gateway, the IP endpoint can connect to any one of the three (3) C-LANs since all connect to the same Gateway.

The last entry in the sample AGL (Note 5 in Figure 22, H.323 Link Bounce recovery process, on page 148) contains the IP address of an Local Survivable Processor (LSP). The single entry implies that there is only one LSP accessible to the endpoint that is hosting the Gateway function.

Anytime the IP endpoint needs to register, it accesses the AGL and tries to register through each C-LAN in succession. If it cannot connect and register with one of the C-LANs, it then attempts to register with a subsequent alternate Gateway in the list. When it reaches the bottom of the list without successfully registering, it continues to cycle through the entire AGL starting from the top. The reaction of the IP endpoint is dependant on whether it is a Softphone or IP Telephone:

- An IP Telephone eventually resets itself and restarts the registration process.
- A Softphone does not perform a reset since the platform on which it is running might not tolerate a reset because other applications are running successfully at the time.

## Maintenance

Maintenance instigates an endpoint audit after a link interruption and on a periodic basis.

## Administration

There are six (6) administration fields associated with the H.323 Link Bounce Recovery mechanism: some related to the Gateway, others for the IP endpoint. All administration is performed in Communication Manager, and those parameters that are destined for the IP endpoint are downloaded when the IP endpoint performs registration and whenever they are changed.

These administration fields are located on two Communication Manager forms:

- IP-Options System Parameters
- IP Network Region

> **NOTE:**
> Registration with a different Gateway could result in different IP endpoint behavior if the parameters are different in the new Gateway.

## IP-Options System Parameters

```
display system-parameters ip-options                                  Page 1 of

                        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

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

| | |
|---|---|
| Field name | Link Loss Delay Timer (min): |
| Values: | 1- 60 |
| Default: | 60 |
| | |
| Field name | Primary Search Time (sec): |
| Values: | 5-3600 |
| Default: | 75 |

**Table 55: Administrable parameters on IP-Options System Parameters form**

| Parameter | Definition |
|---|---|
| H.323 Link Loss Delay Timer [Used within Gateway] | This timer specifies how long the Communication Manager server preserves registration and any stable calls that may exist on the endpoint after it has lost the call signaling channel to the endpoint. If the endpoint does not re-establish connection within this period, Communication Manager tears down the registration and calls (if any) of the endpoint.<br><br>**NOTE:**<br>This timer does not apply to soft IP endpoints operating in telecommuter mode. |
| Primary Search Time [Downloaded to Endpoint] | While the IP Telephone is hung-up, this is the maximum time period that the IP endpoint expends attempting to register with its current Communication Manager server. The need for this timer arises in situations where the current Communication Manager server might have a large number of C-LANs. This timer allows the customer to specify the maximum time that an IP endpoint spends on trying to connect to the C-LANs before attempting to register with an LSP.<br><br>While the IP Telephone's receiver is lifted, the endpoint continues trying to re-establish connection with the current server until the call ends. |

## IP Network Region

```
change ip-network-region 1                                    Page 1 of 19
                           IP NETWORK REGION
  Region: 1
Location:                 Home Domain:
    Name:
                               Intra-region IP-IP Direct Audio: no
AUDIO PARAMETERS               Inter-region IP-IP Direct Audio: no
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3049                      RTCP Reporting Enabled? y
                             RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS      Use Default Server Parameters? y
 Call Control PHB Value: 34                 Server IP Address:   .   .   .
        Audio PHB Value: 46                        Server Port: 5005
802.1P/Q PARAMETERS                  RTCP Report Period(secs): 5
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                    RSVP Enabled? y
   H.323 Link Bounce Recovery? y              RSVP Refresh Rate(secs): 15
 Idle Traffice Interval (sec): 20     Retry upon RSVP Failure Enabled? y
    Keep-Alive Interval (sec): 6               RSVP Profile: guaranteed-service
              Keep-Alive Count: 5     RSVP unreserved (BBE) PHB Value: 40
```

**Table 56: Administrable parameters on IP Network Regions form**

| Parameter | Definition |
|---|---|
| Idle Traffic Interval [Endpoint] | The maximum traffic idle time after which a TCP Keep-Alive (KA) signal is sent from the endpoint. |
| Keep Alive Interval [Endpoint] | The time interval between TCP Keep-Alive re-transmissions. When no ACK is received for all retry attempts, the local TCP stack ends the TCP session and the associated socket is closed. |
| Keep-Alive Count [Endpoint] | The number of times the Keep-Alive message is transmitted if no ACK is received from the peer. |
| H.323 Link Bounce Recovery? | If **y** is entered, the H.323 Link Bounce Recovery feature is enabled for this network region. A **n** disables the feature. [Default is **y**.] |

| | |
|---|---|
| Field name | Idle Traffic Interval (seconds): |
| Values: | 5-7200 |
| Default: | 20 |
| | |
| Field name | Keep-Alive Interval (seconds): |
| Values: | 1-120 |
| Default: | 5 |
| | |
| Field name | Keep-Alive Count: |
| Values: | 1-20 |
| Default: | 5 |

# System resets

The following tables describe the duration, causes, and effects of the S8700 media server's reset levels:

- Reset Level 1 (Warm Restart) on page 153
- Reset Level 2 (Cold-2 Restart) on page 154
- Reset Level 4 on page 155

# Reset Level 1 (Warm Restart)

| | |
|---|---|
| Duration | Up to 10 seconds, typically 4 seconds (**S8100**: 60 seconds) |
| Causes | **reset system 1** command from Communication Manager (SAT/ASA) command line |
| | Spontaneous server interchange (those caused by hardware faults) |
| | Software faults that are not service affecting |
| | Abort of planned server interchange |
| Effects | Stable calls are preserved; queued ACD calls, H.323 calls, and H.320 (multimedia) calls stay up. |
| | System links such as ISDN-PRI D-channel signaling links, CMS, AUDIX, DCS links over C-LAN are preserved. The CMS, DCS, and AUDIX links could lose buffered messages. |
| | Error and alarm logs are preserved, but every alarm is resolved except busyouts. |
| | Stable features are preserved. |
| | Transient calls (not yet connected) and some user stimuli are dropped. |
| | New calls are not processed during the reset. |
| | G3-MT logins, including remote access and system port logins, are dropped. |
| | Every administrative session except those over the TN799 C-LAN are dropped. |
| | If the reset resulted from a spontaneous server interchange, memory shadowing is turned off, and the standby server will not be available for service until memory is refreshed (several minutes). |
| | Application links such as those to AUDIX and CDR are dropped and re-established in under 2½ minutes. |
| | MSS activity is aborted. |
| | Translation data is preserved in memory. If a “save trans” operation is in progress, an SAT-requested warm restart would be aborted. A software-requested warm restart would result in an unsuccessful “save trans” operation and possibly corrupt translations. |

# Reset Level 2 (Cold-2 Restart)

| | |
|---|---|
| Duration | Up to 3.75 minutes (**S8100**: In a large system, up to 5 minutes) |
| Causes | **reset system 2** command from Communication Manager (SAT/ASA) command line |
| | Escalation from SAT's **reset level 1** |
| | An attempted SAT's **reset level 1** during a PNC interchange |
| | Spontaneous interchange into an unrefreshed standby server |
| Effects | **Every system and application link is dropped**. |
| | Every call is dropped. |
| | Every administrative session is dropped. |
| | Every system link is dropped and re-established. |
| | Every application link is dropped and re-established. |
| | Non-translation feature data, such as Automatic Wakeup calls, are lost and must be re-entered. |
| | Translation data is preserved in memory. If a "save trans" operation is in progress, a SAT-requested **cold-2 restart** would be aborted. A software-requested **cold-2 restart** would result in an unsuccessful "save trans" operation and possibly corrupt translations. |
| | Every G3-MT login, including remote access and system port logins, is dropped. |
| | Initialization firmware runs diagnostics and displays results on the G3-MT screen. |
| | Server memory shadowing is turned off, leaving the standby server unavailable for service for up to several minutes. |
| | Every hardware component, except activeTN2312 IPSI in any PN, active EI in a non-IPSI connected PN, SNIs, SNCs, and DS1 clocks. |
| | For a critical-reliability system (duplicated PNC), a global refresh of the standby PNC is performed after the reset. |
| | Every busied-out MO is released and can be rebusied. |
| | Circuit packs are reinitialized. (Translations are verified by comparison to physical boards' locations.) |
| | Error and alarm logs are preserved, and every Communication Manager alarm is resolved. |

## Reset Level 3 (Communication Manager reboot)

This is the same as Reset Level 4 (see below). This command is retained for consistency with other MultiVantage Applications products.

## Reset Level 4

Communication Manager reload

**CAUTION:**
**Reset system 4** leads to an interchange of the system's servers. In response to a level-4 reset, maintenance software downgrades the active server's state of health (SOH), which causes the subsequent interchange.

Once the interchange occurs, the system relies on the previous standby's version of translations, which may not be current. To avoid an unwanted interchange, busy-out the standby server before executing **reset system 4**.

| | |
|---|---|
| Duration | Typically 11 to 14 minutes |
| Causes | **reset system 4** command from Communication Manager (SAT/ASA) command line |
| | Escalation from SAT's **reset level 2** |
| | Power up |
| | Recovery attempt from server-down mode |
| Effects | **S8100**: Emergency Transfer is invoked. |
| | System software (boot image) is reloaded and every process is re-initialized. |
| | Communication Manager processes are reloaded. |
| | Before reboot, the system attempts to save the alarm and error logs. |
| | After reboot, error and alarm logs are restored.<br>Some error and alarm information may be lost if the last save before the reboot save does not succeed. |
| | Other effects are the same as those in reset level 2, except that more extensive diagnostics are performed. |
| | A core dump is automatically enabled for this reset level and is saved to the `/var/log/defty/dumps/` directory. The reboot is delayed until the core dump is finished. |

# Reset Level 5 (Extended Communication Manager reboot)

This is the same as Reset Level 4. This command is retained for consistency with other MultiVantage Applications products.

# S8100 system reset

You can reset the S8100 system from either the web browser interface or the UNIX bash shell from a Telnet session.

## Communication Manager reset (recovery)

There are several less severe resets available to the system that allow it to recover from disrupting errors. These resets can be user initiated with the **reset system *n*** command (where ***n*** is the reset level), and automatically initiated by system software in response to certain error conditions. These commands are used to manually restart the system at various levels, depending on the required test activity. The reset system commands are discussed below.

A system is reset due to a loss of power, or through:

- Reset commands at the administration terminal
- Maintenance software, from which the system can reset itself

  This process starts when certain software and hardware errors are detected by the software.

  **WARNING:**
  When the system is rebooted or reset at level 2, 3, 4, or 5, all voice terminal and attendant console features are adversely affected. Users should be advised of services that are lost and that, as a result, must be reactivated. See System resets on page 152.

The administration terminal display and circuit pack LEDs indicate the progress of the recovery process. See S8300 Media Server LEDs in *Maintenance Alarms Reference (555-245-102)* for more information.

## Non-duplicated SPE

After the reboot command is entered, a series of diagnostics is run on the SPE. Results are displayed as they occur, as described in preceding sections. If every test passes, the boot image is loaded and control is given to the operating system.

If you cannot get the SPE to reboot after replacing the components that failed SPE-down interface tests, follow normal escalation procedures.

# S8300/G700 System reset

There is no change in how Communication Manager functions for system resets in the S8300 Media Server in a G700 Media Gateway. Although translations may be present for a G700, Communication Manager waits for a link to be established before attempting to access the G700. 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 G700 power failure or loss of signaling, Communication Manager detects that the G700 is no longer registered and, after certain conditions are satisfied, begins to remove Media Modules (see Recovery from fatal errors in the S8100 on page 128).

For Media Server resets (as opposed to G700 resets) the G700 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 a system initialization. As a result, the G700 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 a G700 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 G700. 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 “torturing” is set to zero to disable the automatic execution of the command.

### *Results evaluation*

The technician determines the time of the G700 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.

# 6 Troubleshooting

This chapter describes how to resolve problems indicated by alarms and error messages in the system. It includes the following topics:



## Safety precautions

By observing the prescribed safety precautions while working on a system, you can avoid unnecessary damage to its equipment and disruption of service. The items on this list should be a regular part of your routine.

**WARNING:**
Failure to comply with these procedures can have catastrophic effects on a system's hardware and service. Read the explanations following the list to ensure a complete understanding of these necessary procedures.

- While touching any component inside a cabinet, ground yourself using a wrist strap attached to the cabinet's frame, and avoid sources of static electricity.
- When you log on with Avaya Site Administration (ASA), alarm notification is normally disabled. Log off ASA as you leave the system.
- Always busy out a server before you power it down.

- Do ***not*** power down either a switch-node or port carrier to replace a board.
- Handle fiber-optic cables with care. Bending, piercing, or cutting a cable can sever communications between major subsystems.
- To disconnect a fiber-optic cable, grasp both the lightwave transceiver and the cable's connector.
- When you are finished working on a cabinet, replace and secure every panel and cover to avoid disseminating electromagnetic interference.
- Before powering down a cabinet or carrier containing an EMBEDDED AUDIX system (TN568), first power down the AUDIX unit to avoid damaging its software. Instructions for powering down this unit are in Removing and restoring EMBEDDED AUDIX power on page 160, on the circuit pack, and in EMBEDDED AUDIX documentation.

# Removing and restoring EMBEDDED AUDIX power

## Manually power down AUDIX System

A amber caution sticker on the system's power unit notifies technicians to shut down the EMBEDDED AUDIX system prior to powering down the system.

1. Using a pointed object, such as a paper clip or pen (do not use a pencil), press the Boot/Shutdown button. The button is located at the top right portion of the front panel.
2. Hold the Boot/Shutdown button in until the LCD display flashes the message `MSHUT.`
3. Release the Boot/Shutdown button.

**NOTE:**
The EMBEDDED AUDIX system takes about five minutes to shut down. The "heartbeat" indication on the display continues to flash.

## Manually power up AUDIX

1. Using a pointed object such as a paper clip or a pen (do not use a pencil), press the Boot/Shutdown button.
2. Hold the Boot/Shutdown button in until the display indicates the message, `BTEST`, steady on.
3. Release the Boot/Shutdown button. The EMBEDDED AUDIX system takes approximately 5 minutes to power up.

   The display has the following sequence of steady-on messages:

   - OSINIT
   - OS
   - AINIT
   - ADX

   The EMBEDDED AUDIX system is now powered up. When the system is in the active state, the display indicates `ADX`, and the red LED is off.
4. When powering up, the EMBEDDED AUDIX system automatically reboots. This sequence may show an `MD` or `MJ ADX` alarm in the display until the system has powered up. When the system has completed its power-up sequence, the display reads: `ADX`.

## Electrostatic discharge

To avoid system damage or service disruption from ESD while a circuit pack is inserted or removed, attach a grounding wrist strap to the cabinet, and wear it. Also, use a wrist strap while touching any component inside a system's cabinet, (including EMERGENCY TRANSFER switches). Although poor ESD grounding may not cause problems in highly controlled environments, damage or disruption can result in less ideal conditions (for example, when the air is very dry).

If you *must* proceed when a wrist strap is unavailable, grab the outside panel of the cabinet with one hand ***before*** touching any components, and keep your extra hand grounded throughout the procedure.

Handle a circuit pack only by its faceplate, latch, or top and bottom edges. Do not touch a board's components, leads, or connector pins. Keep circuit packs away from plastic and other synthetic materials such as polyester clothing. Do not place a circuit pack on a poorly conductive surface, such as paper. If available, use an anti-static bag.

**WARNING:**

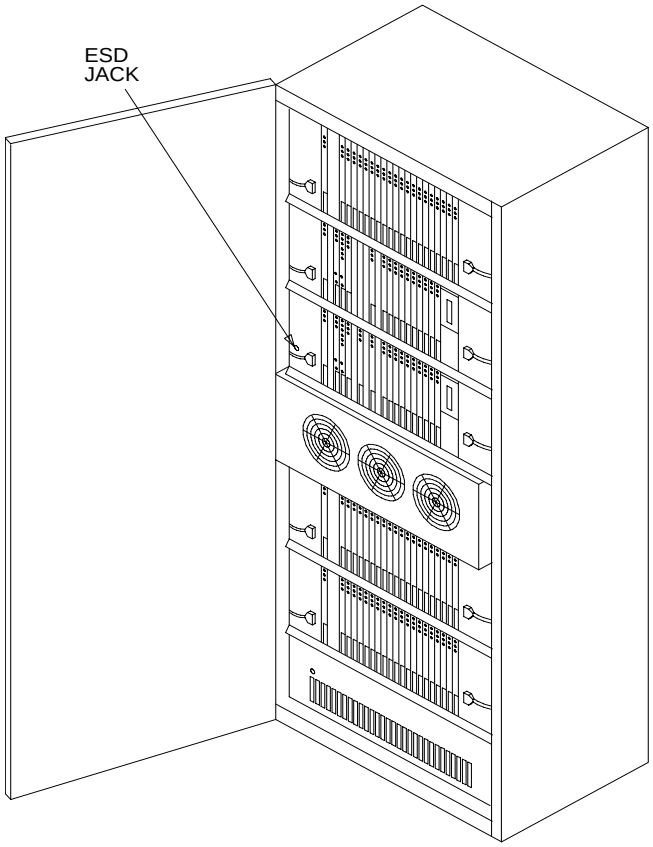
**Never** hand a circuit pack to someone who is **not** also using a grounding wrist strap.

**WARNING:**

People collect potentially damaging amounts of static electricity from many ordinary activities. The smallest amount of ESD we can feel is far above the threshold of damage to a sensitive component or service disruption!

Figure 23, Wrist-strap jack for ESD grounding (MCC1), on page 162 shows the location of the grounding jack.

**Figure 23: Wrist-strap jack for ESD grounding (MCC1)**




# Suppressing alarm origination

While logged in as “craft” to Avaya™ Communication Manager through a:

- Local terminal

  No alarms are reported to Avaya’s alarm receiving system. After logging off, the system automatically resumes alarm origination and reports any unresolved alarms to the alarm receiver.

- Web-based administration process

  The suppression of alarm origination is optional.

Also, while logged in as “craft,” an idle terminal is automatically logged off after 30 minutes. At that time, any unresolved alarms are reported to Avaya’s alarm receiving system. If you are logged in as “craft” at two terminals, the logoff occurs when the second terminal is unused for 30 minutes.

**NOTE:**
The **test inads-link** command functions even if alarm origination is overridden.

# Troubleshooting duplicated servers

The sections, Server initialization, recovery, and resets on page 119, IPSV-CTL (Ipserver Interface Control), and IP-SVR (IP Server Interface) contain procedures for troubleshooting specific problems with servers and IPSIs.

**CAUTION:**
Follow normal escalation procedures **before** shutting down **either** an application or the entire system. Then, execute the shutdown only when advised by the appropriate tier's Services representative.

**CAUTION:**
Communication Manager application resets can have wide-ranging disruptive effects. Unless you are familiar with resetting the system, follow normal escalation procedures before attempting a demand reset.

If a spontaneous server interchange has occurred, assume that a serious fault has occurred on the current standby server. The following symptoms indicate that a spontaneous server interchange has taken place:

- A SYSTEM error is logged in the Error log.
- An interchange entry is recorded in the initcauses log.

The occurrence of a recent interchange is displayed in the Bash shell's **server** screen.

There are two possible causes of a spontaneous interchange:

- Major hardware failure
- Failed recovery that has been software-escalated

If the interchange was fault-driven, there are two ways of finding the cause.

- Using alarm and error logs in conjunction with the timestamp described below.

  After a spontaneous server interchange has occurred, the alarm log retains a record of any MAJOR ON-BOARD alarm against a server component that took place before the interchange. This record is retained for 3 hours and may indicate the cause of the interchange when testing is not possible or conclusive. Other information in the error log may also be helpful.
- Testing the standby server when the logs do not identify the problem.

Start by determining the time of the interchange. (From the server's Bash shell prompt, enter **server**, and refer to the `Elapsed Time Since Last Spont. Interchange` field.) Then, examine the alarm and error logs as described in the following section. If this does not identify the problem, proceed to the next section, which describes a sequence of tests of the standby server.

### Determining the time of a spontaneous interchange

Use **display initcauses** to tell at what time a spontaneous interchange has taken place. The **display initcauses** command displays a record of every system reset. In the following example, a spontaneous interchange into Server B took place at 2:53 p.m. The standby server (B) transitioned into active mode with a WARM restart (reset level 1).

| Cause | Action | Escalated | Carrier | Time |
|---|---|---|---|---|
| Interchange | 1 | no | 1B | 11/27 14:53 |

# Troubleshooting trunks with Automatic Circuit Assurance

A display-equipped voice terminal (may be nondisplay type if the Voice Message Retrieval feature is provided) or an attendant console is required. An “ACA activate/deactivate” button (one per system) is required on the voice terminal or attendant console.

Automatic Circuit Assurance (ACA) assists users in identifying possible trunk malfunctions. The system maintains a record of the performance of individual trunks relative to short and long holding time calls. The system automatically initiates a referral call to an attendant console or display-equipped voice terminal when a possible failure is detected.

Holding time is the elapsed time from when a trunk is accessed to the time a trunk is released. When ACA is enabled through administration, the system measures the holding time of each call.

A short holding time limit and a long holding time limit are preset by the System Manager for each trunk group. The short holding time limit can be from 0 to 160 seconds. The long holding time limit can be from 0 to 10 hours. The measured holding time for each call is compared to the preset limits for the trunk group being used.

Measurements are not made on personal CO lines, out-of-service trunks, or trunks undergoing maintenance testing.

# Using Busy Verification of Terminals and Trunks

A multi-appearance voice terminal or attendant console equipped with a “verify” button is required.

Busy Verification of Terminals and Trunks allows a user at a voice terminal or attendant console to make test calls to trunks, voice terminals, and hunt groups (DDC/UCD). These test calls check the status of an apparently busy resource. This provides an easy method to distinguish between a voice terminal or resource that is truly busy and one that only appears busy because of a trouble condition.

# Trunk Group Busy/Warning Indicators to attendant

An attendant console is required.

Trunk Group Busy/Warning Indicators to Attendant provides the console user with a visual indication of the trunk group status for each trunk group associated with the 12 Trunk Group Select buttons located on the console. Trunk groups with busy indications during nonbusy periods should be checked to ensure that the trunks are busy and not out-of-service. Use the Busy Verification of Terminals and Trunks feature to test the suspected faulty trunks.

# Trunk Identification by attendant

A display-equipped voice terminal or an attendant console equipped with a “trunk id” button is required.

Trunk Identification by Attendant allows a voice terminal or attendant console user to identify a specific trunk being used on a call. This is useful when a user experiences noise or poor transmission on a trunk call. The trunk identification (access code and group number) is displayed when the “trunk id” button is pressed while on a trunk call. Use of this feature is denied if there are more than two trunks on a call. If the call is trunk-to-trunk, the identification displayed is of the last trunk added to the call.

# LA85 port tester

not **S8700**

The LA85 port tester (Comcode 105138424) is recommended for troubleshooting every S8700 Media Server station trouble involving analog, DCP, MFET, MFAT, or BRI configuration. The port tester detects the presence of voltage from equipment ports and indicates the wiring status at the:

- Wall field in the equipment room
- Wall field in any intermediate closet
- Wall jack at the station
- Terminal and its cord

Use the information in Table 57, Port fault isolation using the LA85 port tester, on page 166 to isolate problems with the port tester.

**Table 57: Port fault isolation using the LA85 port tester**

| To begin the isolation procedure at the... | You might need this preliminary information or equipment... | And if... | Then... |
|---|---|---|---|
| Wall field in equipment room | Use **display errors** command | Off-board errors indicated | Verify wiring from switch to equipment room wall field. |
| Station (terminating end) | | | **1** Unplug station cord from terminal and plug it into the “BRI” or “Other” jack on the tester, as applicable.<br>**2** If the readings are OK, the terminal, handset, or handset cord may be faulty. |
| Station wall jack | **1** Wrong or incorrect reading from the terminal end of the station cord<br>**2** D8W line cord (Comcode 103786761) used at station wall jack | | If the reading from the jack is OK, then the terminal cord may be faulty. |
| Intermediate closet wall field | | | Isolate part of the wiring span, either to the switch or to the terminal |

The port tester is equipped to check 110-type wall field hardware with the three 1-pair patch cords that are color-coded blue (1), orange (2), or green (3).

**NOTE:**
If the wall field has 66-type blocks, a 66-type block adapter (Comcode 405546474) is needed.

**DANGER:**
**The port tester should not be plugged into an active circuit for an extended period of time. Resistors in the tester can burn out.**

LED indications for the various port types are listed in Table 58, LED indications for the LA85 port tester, on page 167. Abbreviations are as follows:

- R = Red
- G = Green

- N = Not lighted
- N/A = Not applicable

**Table 58: LED indications for the LA85 port tester**

| Port | W-BL Bl-W | W-O | O-W | W-G | G-W | Bl-W | W-BL |
|---|---|---|---|---|---|---|---|
| Analog | G[1] | N | N | N | N | N/A | N/A |
| DCP | N | G | G | G | G | N/A | N/A |
| DCP (2-wire) | G | N | N | N | N | N/A | N/A |
| MFET | G | G | G | G | G | N/A | N/A |
| MFAT | N | R[2] | R | R | G[3] | N/A | N/A |
| BRI | N/A | N/A | N/A | G | G | G | G |

1 The red LED lights on a reversal. If the analog set contains a polarity guard, the set is still operable. Determine whether off-hook pulls a dial tone that can be broken by dialing.

2 Some LA85 port testers may indicate that W-O should appear green. Information in this chart is correct.

3 Some LA85 port testers may indicate that G-W should appear red. This chart is correct.

# Fiber link fault isolation

Use the following procedure to isolate faults on a fiber link. When troubleshooting a critical-reliability system (duplicated port-network connectivity), first **busyout pnc-standby** before busying out a standby:

- Fiber link (FIBER-LK)
- Expansion Interface (EXP-INTF)
- Switch Node Interface (SNI)
- DS1 Converter (DS1C)

The end of this section describes the pertinent loopback tests and shows a pinout of the cable used to connect the DS1C to DS1 facilities.

**CAUTION:**
Busying out any of these components in a standard-, duplex-, or high-reliability system (nonduplicated PNC) is destructive.

**CAUTION:**
After completing the tests, be sure to release every busied-out component.

Complete the following steps:

1 Enter **display alarms** with category **pnc**.

Are there any on-board alarms? If so, replace the circuit pack(s).

2 Enter **display errors** for category **pnc**.

Check for any of the following errors:

| MO | Error Type |
|---|---|
| FIBER-LK | Any |
| SNI-BD | 513 |
| EXP-INTF | 257–769<br>770,<br>1281,<br>1537,<br>3073,<br>3074,<br>3075,<br>3076,<br>3585,<br>3841,<br>3842 |

If *one or more* of the previous errors are present, proceed with Step 3.

If *not*, look for SNI-PEER errors.

- If there is one SNI circuit pack with many different SNI-PEER error types, replace the indicated SNI circuit pack.
- If there are many SNI-PEER errors with the same error type, replace the indicted SNI circuit pack using the following table.

| Error Type | SNI's Slot |
|---|---|
| 1 | 2 |
| 257 | 3 |
| 513 | 4 |
| 769 | 5 |
| 1025 | 6 |
| 1281 | 7 |
| 1537 | 8 |
| 1793 | 9 |
| 2049 | 13 |
| 2305 | 14 |

*(1 of 2)*

| Error Type | SNI's Slot |
|---|---|
| 2561 | 15 |
| 2817 | 16 |
| 3073 | 17 |
| 3329 | 18 |
| 3585 | 19 |
| 3841 | 20 |
| | *(2 of 2)* |

- After replacing an SNI circuit pack, clear alarms by executing **test board *UUCSS* long clear** for every alarmed EXP-INTF circuit pack. Wait 5 minutes for any SNI-BD or SNI-PEER alarms to clear. To speed this process use **clear firmware counters [a-pnc | b-pnc]** for the PNC that was repaired.
- Exit this procedure.

**3** Enter **list fiber-link** to get the physical location of the fiber link's endpoints. If a DS1 CONV is administered to the fiber link (DS1 CONV is **y**), use the **display fiber-link** command to get the physical location of the DS1 CONV circuit packs on the fiber link.

**4** Execute **busyout fiber-link *FP*,** followed by **test fiber-link *FP* long**.

*If any tests in the sequence fail*, proceed with Step 5.

*If every test passes*, clear alarms by executing **test board *UUCSS* long clear** for every alarmed EXP-INTF circuit pack. Wait 5 minutes for any SNI-BD, SNI-PEER, FIBER-LK, or DS1C-BD alarms to clear. You can speed this process with **clear firmware counters [a-pnc | b-pnc]** for the PNC that was repaired. You are finished with this procedure.

**5** For each of the fiber link's endpoints, follow this flowchart:

**Busyout** and **test board UUCSS long** and record every test failure. When looking at test results, consult the explanations and illustrations of the tests, which appear at the end of this procedure.

Is `Board Not Assigned` displayed for an EXP-INTF in a PN?

- If yes, **test maintenance long** to release an EXP-INTF that may be held reset by a PN's Maintenance circuit pack.
- If No, did EXP-INTF test (#242) fail? If yes, replace the EXP-INTF circuit pack and its lightwave transceiver (if present), and return to Step 4. [The EXP-INTF test (#242) runs an on-board loop around if no lightwave transceiver is connected to the EXP-INTF.]
- If No, did SNI test (#757) fail? If yes, replace the SNI circuit pack, and return to Step 4 of this procedure.
- If No, did SNI test (#756) fail? If yes, replace the SNI circuit pack and its lightwave transceiver (if present), and return to Step 4.
- If No, did EXP-INTF test (#240) fail? If yes, replace the EXP-INTF circuit pack, and return to Step 4.
- If No, did Test #238 (EXP-INTF) or #989 (SNI) fail? If yes, replace the lightwave transceivers and their fiber-optic or metallic cable, and return to Step 4. The faulted component can be further isolated using the Troubleshooting SNI/EI links with manual loop-back on page 171.

**NOTE:**
If a fiber out-of-frame condition exists and lightwave transceivers are used, verify that both lightwave transceivers are the same type, (9823a or 9823b). If not, replace one of the transceivers so that they match. [A 9823A supports distances up to 4900 feet (1493 m), and a 9823B supports distances up to 25,000 feet (7620 m).]

- If No, is a DS1 CONV administered on the fiber link? If no, follow normal escalation procedures.
- If Yes, is there an SNI-BD 513 alarmed error (**display errors,** `category` = pnc)? If yes, replace cabling between the SNI circuit pack and the DS1C circuit pack.
- If the alarm persists, replace the DS1C and the SNI circuit packs, and return to Step 4.
- If No, if the connected circuit pack is an EXP-INTF, did Test #238 fail?

If Yes, replace cabling between the EXP-INTF circuit pack and the DS1C circuit pack. If Test #238 continues to fail, replace the DS1C and the EXP-INTF circuit packs, and return to Step 4.

If No, **busyout** and **test board UUCSS long** for both DS1C circuit packs, and note every test failure or abort.

In a standard-, duplex-, or high-reliability system (nonduplicated PNC), did the test return "`Board not inserted`" for either the near-end circuit pack (nearest the server) or far-end circuit pack? If so, replace the cabling between the DS1C circuit pack and the SNI or EXP-INTF circuit pack.

Wait 1 minute and retest.

If the board is still not inserted, replace the DS1C circuit pack and the EXP-INTF or SNI connected to it, and return to Step 4.

If No, check to see if any of the CSU devices are looped back. **Busyout** and **test ds1-facility UUCSS external-loop** for each DS1 facility. The tests should fail.

If any test passes, the facility is looped back, and the loopback should be removed. If the DS1C complex has only one DS1 facility, this test cannot be executed at the far-end circuit pack (farthest from the server).

Did Test #788 pass and Test #789 fail? If yes, at the other end of the DS1C complex, replace the DS1C and its lightwave transceiver (if present). See Figure 24, Tests for isolating fiber faults, on page 172 and Figure 25, DS1 CONV Loopbacks, on page 172. Return to Step 4.

If No, did Test #788 fail or abort **and** Test #789 fail or abort? If yes, execute **test ds1-facility *UUCSS* long** command for each administered and equipped DS1 facility.

If No, did Test #797 fail?

If Yes, run the **test ds1-facility *UUCSS* external-loopback** command for each administered and equipped DS1 facility.

This test requires manually altering the external connections of the DS1 facility. Place the loopbacks at as many points as your CSU capabilities will allow (see Figure 25, DS1 CONV Loopbacks, on page 172).

- If Test #799 fails at LB1, the problem is with DS1C #1, CSU #1, or the connections in between.
- If Test #799 passes at LB1 but fails at LB2, the problem is with CSU #1.
- If Test #799 passes at both LB1 and LB2, the problem is with the DS1 facility, CSU #2, connections to CSU #2, or DS1C #2.

## Troubleshooting SNI/EI links with manual loop-back

**NOTE:**
Do not use this procedure on a connection with a DS1 CONV as an endpoint.

Use this procedure to isolate a fault in the cables or lightwave transceivers of an SNI/EI link. By performing the loopback at both endpoints and, if applicable, at the cross-connect field, the failure point can be identified. If both endpoints pass but the link remains inactive (with the boards not busied out), the fault should lie in the cabling between. If the test passes at a transceiver but fails at the cross-connect field, the cable or connectors in between are at fault.

A short optical fiber jumper with connectors is required for this procedure. If the link uses metallic cable, the metallic connector must be removed from behind the carrier and a lightwave transceiver connected in its place.

Complete the following steps:

1. Note the condition of the amber LED on the circuit pack.
2. Busyout the circuit pack.
3. Disconnect the transmit and receive fiber pair from the lightwave transceiver behind the circuit pack. Note which is the transmit fiber and which is the receive fiber for proper re-connection at the end of this procedure.
4. Connect the transmit and receive jacks of the lightwave transceiver with the jumper cable.

   **NOTE:**
   Make sure that the total length of the fiber jumper cable does not exceed the maximum length recommended for the fiber link connections between cabinets. Otherwise, test results may be influenced by violation of connectivity guidelines.

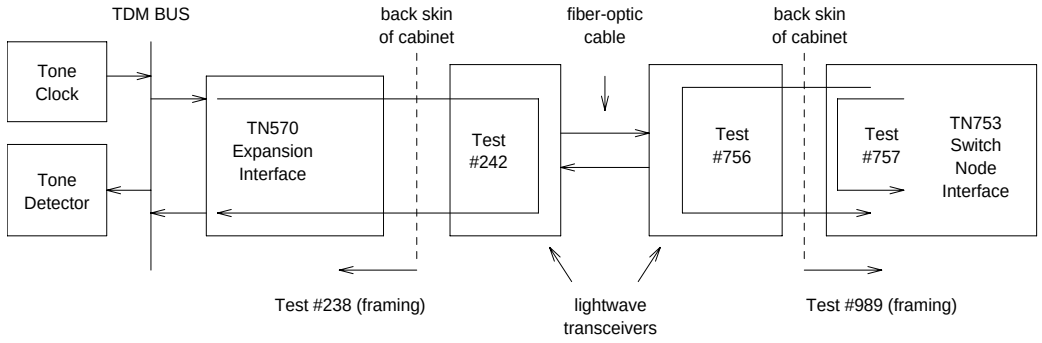
5. At the front of the cabinet, observe the amber LED on the looped back circuit pack.
   - If the amber LED flashes once per second, the circuit pack or transceiver should be replaced.
   - If the amber LED flashes five times per second, the circuit pack or its lightwave transceiver may need replacement. This condition may also be due to a faulty system clock in the PN (for an EI) or in the switch node carrier (for an SNI).
   - If the amber LED was flashing before starting this procedure, and it is now either solid on or solid off, this circuit pack and its lightwave transceiver are functioning properly.
6. Replace the faulty component(s) and reconnect the original cables in their correct positions. Be sure to use a lightwave transceiver that matches the one at the opposite end.
7. Release the circuit pack.

## Isolating fiber faults with loopback tests

Figure 25, DS1 CONV Loopbacks, on page 172 shows the loopbacks performed on the SNI circuit pack for Tests #756 and #757. Test #756 reports the result of the off-board loopback; Test #757 reports the result of the on-board loopback. Tests #756 and #757 can run individually or as part of the **test board *UUCSS* long** command for an SNI circuit pack.

Test #242 can be run as part of the **test board *UUCSS* long** command for an EI circuit pack. Besides testing on-board components, this test is helpful for isolating problems between a circuit pack and the lightwave transceiver. The loopback shown in this diagram shows only part of what Test #242 does. If no lightwave transceiver is connected to the EI circuit pack, an on-board loopback is performed on the EI circuit pack. For more information about Test #242, see EXP-INTF (Expansion Interface Circuit Pack) in *Maintenance Alarms Reference (555-245-102)*.

**Figure 24: Tests for isolating fiber faults**




If DS1-CONVs exist on the fiber link (check with **list fiber-link**), then additional DS1CONV loopback tests can be run to further isolate the problem. The loopback tests are shown in Figure 25, DS1 CONV Loopbacks, on page 172. For more information about DS1-CONV Loopback Tests (#788 and #789), see:

- Far-End DS1 Converter Circuit Pack Loopback Test (#788)
- Far-End Lightwave Transceiver Loopback Test (#789)

For more information about DS1 Facility Loopback tests (#797 and #799), see:

- Far-End Internal Loop-Back Test (#797)
- Near-End External Loop-Back Test (#799)

**Figure 25: DS1 CONV Loopbacks**

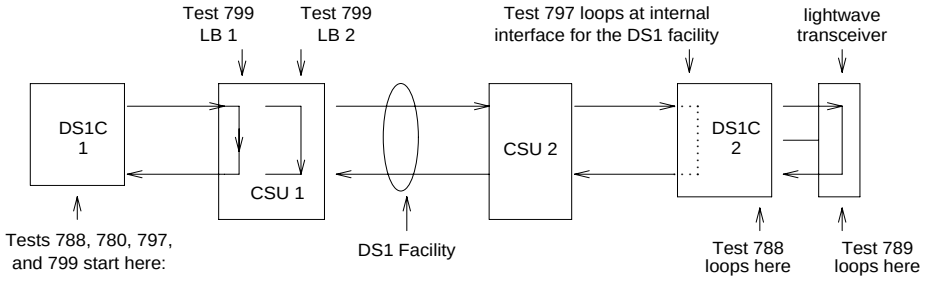



Table 59, DS1 interface cable connectors, on page 173 shows the pin assignments for the cable used to connect the TN574 DS1 CONV circuit pack to DS1 facilities.

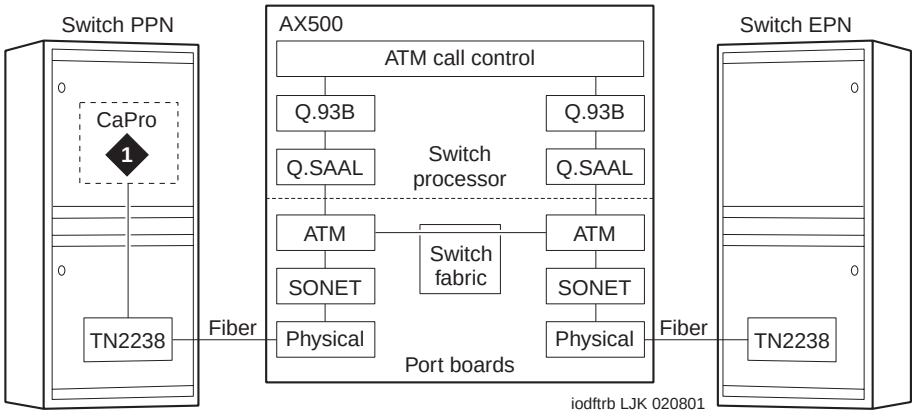
**Table 59: DS1 interface cable connectors**

| Lead | Desig. | 50-pin connector pin | 15-pin connector color | Pin | Color |
|---|---|---|---|---|---|
| Plug 04 | | | | | |
| Facility D Line In | LID | 38 | W-BL | 11 | W-BL |
| Facility D Line In | LID* | 13 | BL-W | 03 | BL-W |
| Facility D Line Out | LOD | 39 | W-O | 09 | W-O |
| Facility D Line Out | LOD* | 14 | O-W | 01 | O-W |
| Plug 03 | | | | | |
| Facility C Line In | LIC | 41 | W-G | 11 | W-G |
| Facility C Line In | LIC* | 16 | G-W | 03 | G-W |
| Facility C Line Out | LOC | 42 | W-BR | 09 | W-BR |
| Facility C Line Out | LOC* | 17 | BR-W | 01 | BR-W |
| Plug 02 | | | | | |
| Facility B Line In | LIB | 44 | W-S | 11 | W-S |
| Facility B Line In | LIB* | 19 | S-W | 03 | S-W |
| Facility B Line Out | LOB | 45 | R-BL | 09 | R-BL |
| Facility B Line Out | LOB* | 20 | BL-R | 01 | BL-R |
| Plug 01 | | | | | |
| Facility A Line In | LIA | 47 | R-O | 11 | R-O |
| Facility A Line In | LIA* | 22 | O-R | 03 | O-R |
| Facility A Line Out | LOA | 48 | R-G | 09 | R-G |
| Facility A Line Out | LOA* | 23 | G-R | 01 | G-R |

# Troubleshooting ATM

This section provides tips for S8700 Multi-Connect ATM PNC when interfacing with the ATM switch. Throughout this section, refer to Figure 26, ATM troubleshooting schematic, on page 174.

**Figure 26: ATM troubleshooting schematic**




**NOTE:**
The CaPro element (Note 1 in Figure 26, ATM troubleshooting schematic, on page 174) is a software module within the S8700 Multi-Connect server.

## Initial LED inspection

Visually inspect the LEDs on both the TN230X (Table 60, TN230X LED reference, on page 174) and the ATM switch (Table 61, A500 LED Quick Reference, on page 175) for a high-level status of the system.

**Table 60: TN230X LED reference**

| LED color | | | |
|---|---|---|---|
| **Red** | **Green** | **Amber** | **Interpretation** |
| Off | Off | Off | Normal state for PN's standby ATM EI board |
| Off | Off | 2 sec on / 2 sec off | Normal state for PN's active PNC archangel ATM EI board |
| – | – | 100ms on / 100ms off | Loss of signal on the OC-3 fiber. Either the TN230X-receive (top) or TN230X-transmit (bottom) fibers are not working. |
| N/S | Fast blink | – | Running DSP diagnostics or downloading code to DSPs (typical during boot process). |
| – | Slow blink | – | Board insertion has not yet completed. |
| – | Steady on | – | Running maintenance tests. May appear to be blinking if several short tests are run one after another. |
| Steady on | – | – | Hardware alarm. Does not necessarily take the TN230X out of service, for example, if one of the 24 DSPs fails diagnostics. |

Table 61, A500 LED Quick Reference, on page 175 shows the various LEDs on the A500 ATM switch and the meanings of the different states.

**Table 61: A500 LED Quick Reference**

| Component | Label | Color | State | Meaning |
|---|---|---|---|---|
| Switch Processor Board | LK | Green | Intermittent blink | Normal state. Traffic is being sent or received over the Ethernet LAN link. |
| | RX | Green | Steady on | Normal state. Carrier is received over the Ethernet LAN link. |
| | DIAG | Green | Off | Normal state. |
| | NBOOT | Green | Off | Normal state. |
| | MGT | Green | Off | Normal state. |
| | RUN | Green | Steady on | Normal state. The switch processor is running. |
| | PWR | Green | Steady on | Normal state. The switch processor board is powered up. |
| | VOLT | Amber | Off | Normal state |
| | TEMP | Amber | Off | Normal state |
| | FAN | Amber | Off | Normal state |
| | SYSERR | Amber | Off | Normal state |
| | FAULT | Amber | Off | Normal state |
| Switch Fabric Board | PWR | Green | Steady on | Normal state. The switch fabric board is powered up. |
| | FAULT | Amber | Off | Normal state |
| Port Board | PWR | Green | Steady on | Normal state. The port board is powered up. |
| | FAULT | Amber | Off | Normal state |

*(1 of 2)*

**Table 61: A500 LED Quick Reference**

| Component | Label | Color | State | Meaning |
|---|---|---|---|---|
| Port Board Per Port | RX | Green | Off | No ATM cells are being received. This is not a normal state if the terminating PN is supposed to be up and running. |
| | RX | Green | Intermitten t blink | ATM cells are being received intermittently. This is a typical pattern if only VBR (variable bit rate) signaling connections are present, but no talk paths are up (perhaps because no calls are in progress). |
| | RX | Green | Steady on | ATM cells are being received frequently enough that the LED is lit constantly. This is a typical pattern if CBR (constant bit rate) talk paths are present. |
| | CD | Green | Off | Loss of carrier on the fiber. The A500 detects only if the A500-receive (right-hand) fiber is not working. The state of the A500-transmit (left hand) fiber is not detected. |
| | CD | Green | Steady on | Normal state. There is a optical carrier detected on the fiber from the TN230X. |
| | RPRD | Amber | Off | Normal state |
| Power Supply | AC OK | Green | Steady on | Normal state. AC power is okay. |
| | DC OK | Green | Steady on | Normal state. DC power is okay. |

*(2 of 2)*

## A500 switch diagnostics

The first step in any diagnostic procedure involving the A500 is to identify the OC-3 ports on the A500 that have S8700 Multi-Connect PNs attached.

- Be aware that customers may use other ports on the A500 for applications unrelated to S8700 Multi-Connect (for example, LAN traffic or multimedia applications).
- These other applications may manifest themselves in the output of the troubleshooting commands you run on the A500. S8700 Multi-Connect PNs must be identified by their A500 port numbers.

**NOTE:**
The following examples show S8700 Multi-Connect PNs connected to A500 ports A1.1 and A1.2.

## Diagnostics

Has the A500 been installed and configured correctly?

- Is the A500 powered up?
- If you are administering the A500 through a locally attached console, is there a local console terminal connected to the console port on the A500 switch processor board with the correctly pinned RS232 serial cable?
- If you are administering the A500 through Telnet over the Ethernet, is there an 10BaseT Ethernet drop plugged into the Ethernet port on the A500 switch processor board? (Note that a few A500 commands are only permitted over the local console terminal.)
- Has the A500 been booted using either the recessed reset button or by turning the power off, then on again?
- Did the A500 go through a normal power-up sequence, including testing every LED?
- Are any A500 amber fault LEDs lit?
- Are the remaining A500 LEDs in a normal state (Table 61, A500 LED Quick Reference, on page 175)?
- Can you log into the A500 console using the diagnostic account **root** from the local console terminal or through Telnet? (See Figure 27, A500 login screen, on page 177.)

**Figure 27: A500 login screen**

```
A500 System Console
                        (c) 1997 Avaya Inc.
login:  root
password:  XXXXXX


********** New System Alarms **********
[1] Failed to fetch configuration files
******* Hit any key to continue *******

A500:
```

**8** Enter **status** at the `A500:` prompt. Figure 28, A500 screen output for status command, on page 178 shows the output from the status command.

**Figure 28: A500 screen output for status command**

```
                    System Status

         A500 System,  Ace_200.01
         Copyright 1996, 1997  Avaya Inc.
         Built Tue Dec 2 08:45:26 EST 1997
         by jdoe in view cm_ace_200
_____________________________________________________

System name              --
System time/date         -- Wednesday, December 3, 1997 15:59:07p
System Uptime            -- days 1,
                         -- hours 1,
                         -- minutes 1
Ethernet IP address      -- 123.1.123.12
Ethernet IP mask         -- 255.255.255.0
LEC IP address           -- 0.0.0.0
LEC IP mask              -- 0.0.0.0
IP default router        -- 123.1.123.123
TFTP server              -- 123.1.123.234
base MAC address         -- 12:34:56:78:9a:bc
ATM address              -- 45.0000.00000123456789abcdef.123456789abc.00
```

**a** If the customer is providing an Ethernet connection to the A500, does the `Ethernet IP address` field have the customer-provided Internet address (configured using the **admin address** command)?

You can administer the A500 through a Telnet connection over the Ethernet, but it is worthwhile making sure the Ethernet address is correct.

**b** If the customer is providing an Ethernet connection to the A500, does the `Ethernet IP mask` field have the customer-provided mask (typically something like `255.255.255.0`, although other values are valid), as configured with the **admin address** command?

**c** If the customer is providing an Ethernet connection to the A500, does the `IP default router` field have the customer-provided Internet address, as configured with the **admin gateway** command?

**d** If the customer is providing an Ethernet connection to the A500 and intends to upload to or download from a TFTP server, does the `TFTP server` field have the customer-provided Internet address, as configured using the **tftp setserver** command?

**e** Does the `ATM address` field have the customer-provided or Avaya-provided network prefix (the first thirteen bytes, set by using the **modify atmprefix** command)?

## ATM administration

Is ATM PNC administered correctly?

**1** Enter **list atm pnc** on the S8700 Multi-Connect's SAT. The cabinet, carrier, and slot positions of each administered TN230X board appear as shown in Figure 29, Screen output for list atm pnc command, on page 179. Ensure that each board's physical location matches the display.

**Figure 29: Screen output for list atm pnc command**

```
list atm pnc                                                Page   1   SPE A
                                ATM PNC
PNC                  A-PNC                    B-PNC
Connection #         LOC                      LOC

 1                   01B02
 2                   02A01
```

You can also use **list configuration *UUC*** (non-control cabinets) to confirm the PN's board locations and correct insertion.

2 Enter **status pnc** at the S8700 Multi-Connect SAT. This screen tells you which TN230X board is active in a duplicated system and how many alarms (if any) of each severity level have been logged for the board. Figure 30, Screen output for status pnc command, on page 179 shows the output from **status pnc**.

**Figure 30: Screen output for status pnc command**

```
status pnc
                          PORT-NETWORK CONNECTIVITY

                                Duplicated? no
                             Software Locked?
                              Standby Busied?

                           Standby Refreshed?
                        Interchange Disabled?

             A-PNC                                    B-PNC

             Mode:  active                             Mode:
   State of Health:                        State of Health:
    Inter PN Index:                         Inter PN Index:

      Major Alarms:  0                         Major Alarms:
      Minor Alarms:  0                         Minor Alarms:
    Warning Alarms:  0                       Warning Alarms:
```

3 Enter either **list configuration *UUC*** (for the carrier where the ATM-EI packs reside) or **display circuit-packs *cabinet*** (non-control cabinet) at the S8700 SAT. This command tells you in more detail what boards are in which slots in each cabinet and carrier. Verify that the TN230Xs are physically located in the slots indicated on the display. Figure 31, Screen output for display circuit-packs 1, on page 180 shows the output for **display circuit-packs 1**. Figure 32, Screen output for display circuit-packs 2, on page 180 shows the output for **display circuit-packs 2**.

**Figure 31: Screen output for display circuit-packs 1**

```
display circuit-packs 1

                              CIRCUIT PACKS

       Cabinet:  1                              Carrier:  A
 Cabinet Layout:  five-carrier            Carrier Type:  processor

         *** PROCESSOR BOARDS NOT ADMINISTERABLE IN THIS SCREEN ***

                              CIRCUIT PACKS

       Cabinet:  1                              Carrier:  B
 Cabinet Layout:  five-carrier            Carrier Type:  port

 Slot Code  Sfx  Name                    Slot Code  Sfx  Name
  00:                                     11:  TN464  C   DS1 INTERFACE
  01:                                     12:  TN464  F   DS1 INTERFACE
  02:  TN2305 ATM PNC EI                   13:  TN767  F   DS1 INTERFACE
  03:                                     14:  TN767  C   DS1 INTERFACE
  04:  TN754  C   DIGITAL LINE             15:  TN760  D   TIE TRUNK
  05:  TN746  B   ANALOG LINE              16:  TN760  D   TIE TRUNK
  06:  TN753      DID TRUNK                17:
  07:  TN771  D   MAINTENANCE/TEST         18:
  08:  TN747  B   CO TRUNK                 19:
  09:  TN556  B   BRI LINE                 20:
  10:  TN767  C   DS1 INTERFACE

  '#' indicates circuit pack conflict.
```

**Figure 32: Screen output for display circuit-packs 2**

```
display circuit-packs 2
                              CIRCUIT PACKS

       Cabinet:  2                              Carrier:  A
 Cabinet Layout:  single-carrier-stack    Carrier Type:  expansion-control

 Slot Code  Sfx  Name                    Slot Code  Sfx  Name
                                          11:  TN746  B   ANALOG LINE
  01:  TN2305 ATM PNC EI                 12:
  02:                                     13:
  03:                                     14:
  04:                                     15:
  05:                                     16:
  06:                                     17:  TN754  C   DIGITAL LINE
  07:
  08:
  09:  TN767  E   DS1 INTERFACE
  10:  TN754  B   DIGITAL LINE

  '#' indicates circuit pack conflict.
```

**4** Enter **display atm pnc *port network*** on the S8700 Multi-Connect SAT.

This display tells you the ATM addresses that have been administered for each TN230X. Verify that each ATM address (the concatenation of the five displayed hexadecimal fields) is correct and match those administered in the A500. See A500 administration on page 182 for more information.

Administered with hard-coded PNNI routes

If the PNs are addressed using *hard-coded PNNI routes* in the A500, the display looks like Figure 33, Screen output for display atm pnc 1, on page 181 (pnc 1) and Figure 34, Screen output for display atm pnc 2, on page 181 (pnc 2).

**Figure 33: Screen output for display atm pnc 1**

```
display atm pnc 1
                                        ATM PNC

                                 Connection Number:  1



      Location:  01B02
          Name:

Address Format:  ICD ATM

             AFI:  47
             ICD:  0005
          HO-DSP:  80FFE1000000F2071B02
             ESI:  000000000000
             SEL:  00
```

**Figure 34: Screen output for display atm pnc 2**

```
display atm pnc 2
                                        ATM PNC

                                 Connection Number:  2



      Location:  02A01
          Name:

Address Format:  ICD ATM

             AFI:  47
             ICD:  0005
          HO-DSP:  80FFE1000000F2072A01
             ESI:  000000000000
             SEL:  00
```

Administered with End System Identifiers

If the PNs are addressed using End System Identifiers (ESIs), the display looks like Figure 35, Screen output for display atm pnc 1 with End System Identifiers, on page 182 (pnc 1) and Figure 36, Screen output for display atm pnc 2 with End System Identifiers, on page 182 (pnc 2).

**Figure 35: Screen output for display atm pnc 1 with End System Identifiers**

```
display atm pnc 1
                                        ATM PNC

                                 Connection Number:  1

              A - PNC
          Location:  01B02
              Name:

Address Format:  E.164 ATM Private

               AFI:  45
             E.164:  0001013035381053
            HO-DSP:  00000000
               ESI:  000000000011
               SEL:  00
```

**Figure 36: Screen output for display atm pnc 2 with End System Identifiers**

```
display atm pnc 2
                                        ATM PNC

                                 Connection Number:  2

              A - PNC

          Location:  02A01
              Name:

Address Format:  E.164 ATM Private

               AFI:  45
             E.164:  0001013035381053
            HO-DSP:  00000000
               ESI:  000000000012
               SEL:  00
```

## A500 administration

Is the A500 administered correctly?

1 Enter **show signaling summary** on the A500 console. Figure 37, Screen output for the show signaling summary command, on page 183 shows the screen output.

**Figure 37: Screen output for the show signaling summary command**

```
A500:show signaling summary

Port    loc VCI   SAP   IntType    Signaling   ILMI  SAP State     State
------  -------   ---   -------   -----------  ----  ------------  -----
A1.1     1        1     Network   UNI3.1       No    UP            UP
A1.2     2        2     Network   UNI3.1       No    UP            UP
```

**a** If an A500 port with an attached S8700 Multi-Connect PN is not listed in this display, it is likely that the port was administered incorrectly as having no UNI signaling (**admin link** command).

Ensure that fields listed have the following values.

| Field | Value |
|---|---|
| `IntType` | `Network`<br>If it is `User`, links will not come up between the PNs. |
| Signaling | UNI3.1<br>If it is `UNI3.0`, links will not come up between the PNs. |
| ILMI | Preferred value of is `No`, however this alone does not prevent links from coming up between the PNs. |
| SAP State | May or may not be `UP`. Their values depend on more than just whether the port was marked as **UP**. (See highlighted data for SAP State in Figure 37, Screen output for the show signaling summary command, on page 183.) |

**2** If the A500 was administered using hard-coded PNNI routes to identify each endpoint, enter **show signaling routes** on the A500 console.
Figure 38, Screen output from the show signaling routes command, on page 183 shows the screen output from the command.

**Figure 38: Screen output from the show signaling routes command**

```
A500:show signaling routes

Number of Local Static Routes Allowed:  30
Current number of Local Static Routes:  2

Address:  47.00.05.80.ff.e1.00.00.00.f2.07.2a.01.00.00.00.00.00.00.00
mask:152  cost:   0  node:self  port:A1.2 state:UP

Address:  47.00.05.80.ff.e1.00.00.00.f2.07.1b.02.00.00.00.00.00.00.00
mask:152  cost:   0  node:self  port:A1.1 state:UP
```

Check that the `Address` field (administered using the **admin signaling route add** command) matches those administered in S8700 Multi-Connect.

3 If the A500 was administered using End System Identifiers, enter **show signaling esi** on the A500 console. Figure 39, Screen output A500: show signaling esi command, on page 184 shows the command output.

**Figure 39: Screen output A500: show signaling esi command**

```
A500:show signaling esi
Addresses registered on A1.1
----------------------------
* 45.0001.0130353810530000000.000000000011.00

Addresses registered on A1.2
----------------------------
* 45.0001.0130353810530000000.000000000012.00

( * - configured )
```

Check that the `Addresses registered` (use the **admin signaling esi add** command) match those administered in S8700 Multi-Connect.

- If an address or End System Identifier is missing or incorrect on the A500 port associated with the IPSI-connected PN, the EAL and PACL links will come up, but 1-way talk paths may result. (The ATM network can route from the IPSI-connected PN to another PN, which creates the bidirectional EAL and PACL signaling channels and one side of the talk path.)
- If an address or End System Identifier is missing or incorrect on the A500 port associated with a non-IPSI-connected PN, the links will not come up between the PN and its controlling IPSI-connected PN.

4 Enter **show sys interfaces** on the A500 console. Figure 40, A500 screen output for show sys interfaces command, on page 185 shows the screen output.

**Figure 40: A500 screen output for show sys interfaces command**

```
Device    Oper      Admin     State      Type
          Status    Status
_____________________________________________________________________
A1.1      up        up        present    STS_3c (MultiMode)
A1.2      up        up        present    STS_3c (MultiMode)
A1.3      down      down      present    STS_3c (MultiMode)
A1.4      down      down      present    STS_3c (MultiMode)
A1.5      down      down      present    STS_3c (MultiMode)
A1.6      down      down      present    STS_3c (MultiMode)
A1.7      down      down      present    STS_3c (MultiMode)
A1.8      down      down      present    STS_3c (MultiMode)
A2.1      down      down      present    STS_3c (MultiMode)
A2.2      down      down      present    STS_3c (MultiMode)
A2.3      down      down      present    STS_3c (MultiMode)
A2.4      down      down      present    STS_3c (MultiMode)
A2.5      down      down      present    STS_3c (MultiMode)
A2.6      down      down      present    STS_3c (MultiMode)
A2.7      down      down      present    STS_3c (MultiMode)
A2.8      down      down      present    STS_3c (MultiMode)
A3.1      down      down      invalid    STS_3c (MultiMode)
A3.2      down      down      invalid    STS_3c (MultiMode)
A3.3      down      down      invalid    STS_3c (MultiMode)
A3.4      down      down      invalid    STS_3c (MultiMode)
A3.5      down      down      invalid    STS_3c (MultiMode)
A3.6      down      down      invalid    STS_3c (MultiMode)
A3.7      down      down      invalid    STS_3c (MultiMode)
A3.8      down      down      invalid    STS_3c (MultiMode)
A4.1      down      down      invalid    STS_3c (MultiMode)
A4.2      down      down      invalid    STS_3c (MultiMode)
A4.3      down      down      invalid    STS_3c (MultiMode)
A4.4      down      down      invalid    STS_3c (MultiMode)
A4.5      down      down      invalid    STS_3c (MultiMode)
A4.6      down      down      invalid    STS_3c (MultiMode)
A4.7      down      down      invalid    STS_3c (MultiMode)
A4.8      down      down      invalid    STS_3c (MultiMode)
Self      up        up        present    PROPVIRTUAL
Self      up        up        present    SAR
E1.1      up        up        present    TenBaseT
```

- For each administered port used by a S8700 Multi-Connect port network, the `Admin Status` should be `up` (using the **admin up** command).
- The state of `Oper Status` is not pertinent to administration of the A500 and is discussed under Figure 46, A500: show sys interfaces, on page 189.
- `State` should be `present`, indicating that A500 port board insertion was successful. If `State` is `invalid`, then the A500 believes that the corresponding port board slot is empty or the port board is not recognized.

  It may be necessary to re-administer the A500 port boards. Refer to the *Cajun A500 Quick Reference* for further information.
- If `Admin Status` or `State` is incorrect, the links will not come up between a non-IPSI-connected PN and its controlling IPSI-connected PN.

# TN230X circuit pack(s)

Did the TN230X come up correctly?

1. Review the LED conditions for the TN230X:
   - Do the TN230X LEDs (see Table 60 on page 174) indicate a normal operational state (any of the following):
     - — Archangel mode in the PN
     - — Standby in the PN
2. If after board insertion or a demand reset:
   - Do the TN230X LEDs indicate that it is booting?
   - Do the TN230X LEDs indicate it is downloading its DSPs?
   - Do the TN230X LEDs indicate that board insertion has not yet occurred?
   - Do the TN230X LEDs indicate a maintenance alarm?
3. Enter **list configuration carrier *cabinet carrier*** on the S8700 Multi-Connect SAT. See the following Figure 41, List configuration carrier 1b screen, on page 186 (1b) and Figure 42, List configuration carrier 2a screen, on page 187 (2a).

**Figure 41: List configuration carrier 1b screen**

```
list configuration carrier 1b

                              SYSTEM CONFIGURATION

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

01B02     ATM PNC EI               TN2305 000001
01B04     DIGITAL LINE             TN754C  000002     u  u  u  u  u  u  u  u
01B05     ANALOG LINE              TN746B  000010     u  u  u  u  u  06 u  u
                                                      u  u  u  u  u  u  u  u
01B06     DID TRUNK                TN753   000021     u  u  u  u  u  u  u  u
01B07     MAINTENANCE/TEST         TN771D  000006     u  02 03 04
01B08     CO TRUNK                 TN747B  000018     u  u  u  u  u  u  u  u
01B09     BRI LINE                 TN556B  000003     u  u  u  u  u  u  u  u
                                                      u  u  u  u  u  u  u  u
                                                      u  u  u  u  u  u  u  u
01B10     DS1 INTERFACE            TN767C  000003     u  u  u  u  u  u  u  u
                                                      u  u  u  u  u  u  u  u
                                                      u  u  u  u  u  u  u  u
```

**Figure 42: List configuration carrier 2a screen**

```
list configuration carrier 2a

                              SYSTEM CONFIGURATION

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

02A01    ATM PNC EI               TN2305 000001
02A09    DS1 INTERFACE            TN767E  000004     u  u  u  u  u  u  u  u
                                                     u  u  u  u  u  u  u  u
                                                     u  u  u  u  u  u  u  u
02A10    DIGITAL LINE             TN754B  000016     u  u  u  u  u  u  u  u
02A11    ANALOG LINE              TN746B  000010     01 u  u  u  u  u  u  u
                                                     u  u  u  u  u  u  u  u
02A17    DIGITAL LINE             TN754C  000002     u  u  u  u  u  u  u  u
```

- The TN230X board should be shown in the correct slot.
- Fields should have the following indicated values:

| Field | Value |
|---|---|
| Board Type | ATM PNC EI |
| Vintage | The TN230X vintage. If Vintage is no board, then either the board is in the incorrect slot or board insertion was not completed correctly. Refer to Reseating and replacing circuit packs on page 277. |

**4** If the TN230X is inserted and shows a vintage number, enter **test board** ***cabinetcarrierslot*** for this board on the S8700 Multi-Connect SAT, as shown in Figure 43, Screen output for the test board 1b02 command, on page 187 (1b02) and Figure 44, Screen output for the test board 2a01 command, on page 188 (2a01).

**Figure 43: Screen output for the test board 1b02 command**

```
test board 1b02

                                TEST RESULTS

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

  01B02     ATM-EI                      316      PASS
  01B02     ATM-EI                      598      PASS
  01B02     ATM-EI                      1258     PASS
  01B02     ATM-EI                      241      PASS
  01B02     ATM-EI                      304      PASS
  01B02     ATM-EI                      1259     PASS
```

**Figure 44: Screen output for the test board 2a01 command**

```
test board 2a01

                                TEST RESULTS

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

  02A01     ATM-EI                      316      PASS
  02A01     ATM-EI                      598      PASS
  02A01     ATM-EI                      1258     PASS
  02A01     ATM-EI                      241      PASS
  02A01     ATM-EI                      304      PASS
  02A01     ATM-EI                      1259     PASS
```

- The `Result` should be PASS for each test number. If any of the tests fail, refer to ATM-BCH (ATM B-Channel Trunk).

### Possible Causes

1. The TN230X board is in a slot different from the S8700 Multi-Connect administration.
2. The TN230X did not complete board insertion.

## Physical layer

Is there an optical signal between the TN230X and the A500?

1. Does the TN230X's amber LED flash 100ms on/100ms off, indicating a loss of signal on the fiber? Recall that the TN230X detects continuity problems with either the Transmit (bottom) or the Receive (top) fibers.

   If there is loss of signal on the fiber, refer to Fiber link fault isolation on page 167.
2. Is the A500 port's CD LED off, indicating a loss of signal on the fiber? Note that the A500 detects continuity problems only with the Receive (right-hand) fiber; the state of the Transmit (left-hand) fiber is not detected.
3. Enter **show signaling summary** on the A500 console. Figure 45, A500: show signaling summary screen, on page 188 shows the screen output.

**Figure 45: A500: show signaling summary screen**

```
A500:show signaling summary

Port    loc VCI   SAP   IntType    Signaling   ILMI  SAP State     State
------  -------   ---   -------   -----------  ----  ------------  -----
A1.1      1       1     Network   UNI3.1       No    UP            UP
A1.2      2       2     Network   UNI3.1       No    UP            UP
```

Ensure that the fields have the following indicated values.

| | |
|---|---|
| SAP State | Up<br>If it is PHY_DOWN or DOWN, there may be a loss of signal on the port in question. This command detects a continuity problem only with the Receive (right-hand) fiber. It does not detect the state of the Transmit (left-hand) fiber. |
| State | The value may be UP or DOWN, depending on the administration of the port. It may be necessary to re-administer the A500 port boards. Refer to the *Cajun A500 Quick Reference* for further information. |

**4** Enter **show system interfaces** on the A500 console. Figure 46, A500: show sys interfaces, on page 189 shows an example of the screen output.

**Figure 46: A500: show sys interfaces**

```
Device    Oper      Admin     State      Type
          Status    Status
_____________________________________________________________________
A1.1      up        up        present    STS_3c (MultiMode)
A1.2      up        up        present    STS_3c (MultiMode)
A1.3      down      down      present    STS_3c (MultiMode)
A1.4      down      down      present    STS_3c (MultiMode)
A1.5      down      down      present    STS_3c (MultiMode)
A1.6      down      down      present    STS_3c (MultiMode)
A1.7      down      down      present    STS_3c (MultiMode)
A1.8      down      down      present    STS_3c (MultiMode)
A2.1      down      down      present    STS_3c (MultiMode)
A2.2      down      down      present    STS_3c (MultiMode)
A2.3      down      down      present    STS_3c (MultiMode)
A2.4      down      down      present    STS_3c (MultiMode)
A2.5      down      down      present    STS_3c (MultiMode)
A2.6      down      down      present    STS_3c (MultiMode)
A2.7      down      down      present    STS_3c (MultiMode)
A2.8      down      down      present    STS_3c (MultiMode)
A3.1      down      down      invalid    STS_3c (MultiMode)
A3.2      down      down      invalid    STS_3c (MultiMode)
A3.3      down      down      invalid    STS_3c (MultiMode)
A3.4      down      down      invalid    STS_3c (MultiMode)
A3.5      down      down      invalid    STS_3c (MultiMode)
A3.6      down      down      invalid    STS_3c (MultiMode)
A3.7      down      down      invalid    STS_3c (MultiMode)
A3.8      down      down      invalid    STS_3c (MultiMode)
A4.1      down      down      invalid    STS_3c (MultiMode)
A4.2      down      down      invalid    STS_3c (MultiMode)
A4.3      down      down      invalid    STS_3c (MultiMode)
A4.4      down      down      invalid    STS_3c (MultiMode)
A4.5      down      down      invalid    STS_3c (MultiMode)
A4.6      down      down      invalid    STS_3c (MultiMode)
A4.7      down      down      invalid    STS_3c (MultiMode)
A4.8      down      down      invalid    STS_3c (MultiMode)
Self      up        up        present    PROPVIRTUAL
Self      up        up        present    SAR
E1.1      up        up        present    TenBaseT
```

`Oper Status` should be `up`. If it is `down`, there is likely a loss of signal on the port in question (`State` of `present`), or the A500 does not recognize the port board (`State` of `invalid`). This command detects a continuity problem only with the Receive (right-hand) fiber; it does not detect the state of the Transmit (left-hand) fiber.

### Possible causes

- The fiber is disconnected from the A500 and/or the TN230Xs.
- The Transmit and Receive fibers are swapped at the A500 or the TN230X (but not both).
- There is a break in the fiber.
- The TN230X is not transmitting a carrier signal (not inserted, not powered, or not administered). See ATM-BCH (ATM B-Channel Trunk).
- If no carrier signal is received, an optical transceiver's hardware-safety interlocks may cut transmission power. So, a transmission problem could indicate an unreceived carrier signal at the same end.
- The A500 does not recognize that there is a port board in the slot. It may be necessary to re-administer the A500 port boards. Refer to the *Cajun A500 Quick Reference* for further information.

### Recommended action

1. Plug in, swap, repair, or replace the fiber as necessary.
2. Verify that the port board is inserted.

## SONET layer

Are SONET frames reaching the A500?

Is the A500 port's green RX LED solid off, indicating no cell traffic?

1. Enter **show stats sonet *port*** on the A500 console. Figure 47, A500: show stats sonet a1.2 screen, on page 191 shows the screen output.

   **NOTE:**
   The following examples point to port A1.2 as the port of interest.

**Figure 47: A500: show stats sonet a1.2 screen**

```
    Sonet per-Port Statistics
--------------------------------

 Receive Cell Count:      80654
 Transmit Cell Count:     79555

 Section Level Bit Err:   1
 Line Bit Err:            1
 Line FEB Err:            168
 Path Bit Err:            1
 Path FEB Err:            98
 Correctable HCS Err:     0
 Uncorrectable HCS Err:   0
 Loss of Frame Err:       1
 Loss of Signal Err:      0
 Out of Frame Err:        0

 Path Signal Label:       19
```

**2** Ensure that the fields have the following indicated values.

| | |
|---|---|
| `Receive Cell Count` | Each field's values should be increasing if the TN230X is actively sending and receiving cells with the A500. (Even if a TN230X did not achieve board insertion, it will still try to talk to the A500.) |
| `Transmit Cell Count` | If neither field is increasing, the A500 port might have been marked down using **admin down**. Use **show system interfaces** to verify that the `Admin Status` is up.<br><br>If the `Receive Cell Count` is increasing but the `Transmit Cell Count` is not increasing, this may be because the port was administered with no UNI signaling (**admin link** command). Use **show signaling summary** to ensure that `Signaling` is `UNI3.1`.<br><br>The error counters might not be zero, but should not be large either compared to the receive and transmit cell counters. If the counters are large and increasing, check the fiber integrity. Make sure the fiber pairs are securely plugged into both the TN230X and the A500.<br><br>If the fiber has been pulled and reinserted as part of fault diagnosis, the non-zero `Loss of Signal Err` counter might be correct. |

## Q.SAAL (data link) layer

Are ATM signaling messages reaching A500 Call Control?

Enter **show signaling stats *port* qsaal** on the A500 console. Figure 48, A500: show signaling stats a1.2 qsaal screen, on page 192 shows the screen output.

**Figure 48: A500: show signaling stats a1.2 qsaal screen**

```
A500:  show signaling stats a1.2 qsaal

------------------------Q.SAAL Statistics-----------------------
Port A1.2:
----------
Type:  UNI3.1
VPI:  0x00, VCI:  0x05
                        Tx          Rx
                    --------    --------
BGN PDUs:                 0           1
BGAK PDUs:                1           0
END PDUs:                 0           0
ENDAK PDUs:               0           0
RS PDUs:                  0           0
RSAK PDUs:                0           0
BGREJ PDUs:               0           0
SD PDUs:                 81          78
SDP PDUs:           Supported only for UNI 3.0
ER PDUs:                  0           0
POLL PDUs:             6259        5720
STAT PDUs:             5720        6259
USTAT PDUs:               0           0
ERAK PDUs:                0           0
Discarded PDUs:           0           0
Errored PDUs:             0           0
Buffers in use:           0           0
High buffer mark:         3           0
```

**NOTE:**
If there is no connection between the TN230X and the A500 at the Q.SAAL protocol layer, then no report is displayed.

— If `Port A1.2` (or the port of interest) is `not configured for UNI signaling`, then the port was administered for no UNI signaling (**admin link** command). Use the **show signaling summary** command to verify that `Signaling` is `UNI3.1`.

— The `Supported only for UNI 3.0` line for the `SDP PDUs:` field means that the port was administered for UNI3.0 signaling (**admin link** command). Use the **show signaling summary** command to verify that `Signaling` is `UNI3.1`.

— The `POLL PDUs` and `STAT PDUs` counters should be increasing if the TN230X is actively sending and receiving Q.SAAL Protocol Data Units with the A500. This occurs even if the TN230X did not achieve board insertion.

## Q.93B (network) layer

Are connection requests being received by A500 Call Control?

1 Enter **show signaling stats *port* q93b** (or the port of interest) on the A500 console. Figure 49, A500:show signaling stats A1.2 q93b, on page 193 shows the screen output.

**Figure 49: A500:show signaling stats A1.2 q93b**

```
A500:show signaling stats a1.2 q93b

------------------------Q.93B Statistics-----------------------
Port A1.2:
----------
                        Tx          Rx
                    --------    --------
Connect Messages:         15          18
Setup Messages:           18          15
Release Messages:         17          13
Rel Cmplt Messages:       13          17
Add Party Messages:        0           0
Add Party Acks:            0           0
Add Party Rejects:         0           0
Drop Party Messages:       0           0
Drop Party Acks:           0           0
Last Cause Code:          31          31
Last Diag Code:      0. 0. 0    71. 0.29
Total Connections:        33
Current Connections:       3
```

**NOTE:**
If there is no connection between the TN230X and the A500 at the Q93B protocol layer, then no report displays.

**2** Ensure that the fields have the following indicated values.

| | |
|---|---|
| `Port A1.2` (or the port of interest) | If this field is `not configured for UNI signaling`, then the port was administered for no UNI signaling (**admin link** command). Use the **show signaling summary** command to verify that `Signaling` is `UNI3.1`. |
| `Connect Messages`<br>`Setup Messages`<br>`Release Messages` | These counters should be non-zero if the A500 is handling Q.93B protocol layer messages sent by the PPN and PN. They may not increase during troubleshooting unless calls are being made, since the PPN initially sets up control connections to the PPN and then sets up talk path connections as needed. |

**3** If connections are being rejected, the `Last Cause Code` may suggest why. The cause code (in following Table 62, Observed cause codes, on page 195) indicating the error may be on the PPN port even though the PN port is the one misbehaving, and vice versa.

Enter **show signaling cause *causecode*** on the A500 console. Figure 50, A500:show signaling cause 31, on page 194 shows the screen output for this command.

**Figure 50: A500:show signaling cause 31**

```
A500:show signaling cause 31

Cause 31:  Normal, unspecified
```

**4** At the S8700 Multi-Connect SAT type **display errors**, and press Enter.

Set the `Error List` to **errors** and `Category` to **PNC** on the input screen (Figure 51, S8700 Multi-Connect display errors input screen, on page 194), and press Enter to display any cause codes (see following Table 62, Observed cause codes, on page 195) returned from the ATM network to a TN230X on the PPN (and to a TN230X in a PN). This is successful only if the links between the PPN and the PN remain up so that the message from the PN is logged.

Refer to ATM-BCH (ATM B-Channel Trunk) for detailed information about cause codes for this MO.

**Figure 51: S8700 Multi-Connect display errors input screen**

```
display errors                                    Page   1 of   1   SPE A
                                ERROR REPORT

      The following options control which errors will be displayed.
         ERROR TYPES

            Error Type:               Error List:  errors


         REPORT PERIOD

            Interval:  a      From:   /  /  :   To:   /  /  :

         EQUIPMENT TYPE ( Choose only one, if any, of the following )

                              Cabinet:
                         Port Network:
                         Board Number:
                                 Port:
                             Category:  PNC
                            Extension:
                  Trunk ( group/member ):    /
```

Figure 52, Screen output for display errors command, on page 195 shows the screen output for the **display errors** command.

**Figure 52: Screen output for display errors command**

```
display errors                                          Page   9   SPE A

                            HARDWARE ERROR REPORT

Port     Mtce    Alt    Err  Aux    First      Last     Err Err Rt/ Al Ac
         Name    Name   Type Data   Occur      Occur    Cnt Rt  Hr  St

AT01A    ATM-NTWK       41   1    11/12/16:59 12/09/15:10 14  0   0   n  n
AT01A    ATM-NTWK       31   0    11/13/18:27 11/20/20:02 5   0   0   n  n
AT02A    ATM-NTWK       0    0    11/13/18:45 11/13/18:45 1   0   0   n  n
AT02A    ATM-NTWK       31   0    11/15/14:40 11/15/14:41 2   120 0   n  n
AT01B    ATM-NTWK       31   0    11/16/17:39 11/16/17:39 1   0   0   n  n
AT01A    ATM-NTWK       3    1    11/16/18:19 11/26/13:13 12  0   0   n  n
```

In this example the errors that have `ATM-NTWK` for `Name` and `1` for `Data` indicate an error returned to the TN230X from the ATM network. In this case, `Type` indicates the cause code returned by the ATM network (see Table 62, Observed cause codes, on page 195). In the previous example, two cause codes (41 and 3) are reported from the ATM network. For more information about these cause codes and repair information see ATM-NTWK (ATM Network Error).

**Table 62: Observed cause codes**

| Cause code | Definition | Observed cause |
|---|---|---|
| 3 | No route to destination | The ATM addresses administered in the ATM switch (**show signaling routes** or **show signaling esi**) or in the S8700 (**display atm pnc**) are incorrect. |
| 31 | Normal, unspecified | This is a normal return. |
| 41 | Temporary failure | This “try again later” cause code has been observed when the source of the problem is on another port (for example, a routing problem on another port that displays cause code 3). |
| 47 | Resources unavailable, unspecified | S8700 call volume is too high for the available resources in the ATM network. |
| 63 | Service or option unavailable, unspecified | S8700 call volume is too high for the available resources in the ATM network. |

## ATM call control

Are ATM signaling connections being setup to A500 Call Control?

Enter **show switch circuit table** on the A500 console. Figure 53, A500: show switch circuit table screen, on page 196 shows the screen output.

**Figure 53: A500: show switch circuit table screen**

```
A500:show switch circuit table

 ____________________________________________________________
|    Input      |    Output     |       Connection           |
| port vpi  vci| port vpi  vci| type class  parameters       |
|______________|______________|____________________________|

  A1.1   0    5  Self   0    1  pp   UBR    ppd on
  A1.1   0   32  A1.2   0   32  pp   VBRnrt pcr=5729  /scr=5729  /mbs=17187
  A1.1   0   35  A1.2   0   35  pmp  CBR    pcr=173

  A1.2   0    5  Self   0    2  pp   UBR    ppd on
  A1.2   0   32  A1.1   0   32  pp   VBRnrt pcr=5729  /scr=5729  /mbs=17187
  A1.2   0   34  A1.1   0   34  pmp  CBR    pcr=173

  Self   0    1  A1.1   0    5  pp   UBR    ppd on
  Self   0    2  A1.2   0    5  pp   UBR    ppd on
 ____________________________________________________________
```

- The `pp UBR` virtual circuits between A500 ports `A1.1` (PPN) and `Self` (A500) and between `A1.2` (PN) and `Self` (A500) are ATM signaling channels between the port network and the A500.
- They are used to request connection setups and releases to other endpoints such as another port network.
- These are established by each TN230X when it comes up, independent of S8700 call processing.
- Other UBR virtual circuits may exist between A500 ports that are not associated with S8700 port networks and may be signaling channels for other applications (for example, data network traffic).

# CaPro layer

**Are control channels being established from the PPN to a PN?**

## Diagnostics

- Do you get a dial tone from a set on the PN in question?
- Can you ring a set on this PN dialing from the PPN, and vice versa?

Complete the following steps:

1. Enter **list sys-link** on the S8700 Multi-Connect SAT. Figure 54, List sys-link screen, on page 197 shows the screen output.

**Figure 54: List sys-link screen**

```
list sys-link

                          SYSTEM LINKS INFORMATION

Location  Link Type/     State   Current      Faulted    Last Fault
          Channel                Path         Path       Recorded

02A0101   EAL           up      present      present    12/06/1997 16:20
01B0202   PACL          up      present      present    12/06/1997 16:17
02A0102   PACL          up      present      present    12/06/1997 16:20
```

Ensure that the fields have the following indicated values.

| | |
|---|---|
| `Link Type/ Channel` | One `PACL` to each TN230X in either a PPN or a PN, and one `EAL` to each TN230X in a PN. |
| `State` | `up` |

2 Enter **show switch circuit**

3 **Enter table** on the A500 console. Figure 55, A500: show switch circuit screen, on page 197 shows the screen output.

**Figure 55: A500: show switch circuit screen**

```
A500:show switch circuit
 ____________________________________________________
|    Input     |    Output    |       Connection       |
| port vpi  vci| port vpi  vci| type class  parameters |
|______________|______________|________________________|

  A1.1   0    5  Self   0    1  pp   UBR    ppd on
  A1.1   0   32  A1.2   0   32  pp   VBRnrt pcr=5729  /scr=5729  /mbs=17187
  A1.1   0   35  A1.2   0   35  pmp  CBR    pcr=173

  A1.2   0    5  Self   0    2  pp   UBR    ppd on
  A1.2   0   32  A1.1   0   32  pp   VBRnrt pcr=5729  /scr=5729  /mbs=17187
  A1.2   0   34  A1.1   0   34  pmp  CBR    pcr=173

  Self   0    1  A1.1   0    5  pp   UBR    ppd on
  Self   0    2  A1.2   0    5  pp   UBR    ppd on
____________________________________________________
```

- The pp VBRnrt (Variable Bit Rate) virtual circuits between A500 ports A1.1 (PPN) and A1.2 (PN) are used for signaling between the PPN and each PN.
- These are established once upon initialization under control of S8700 Multi-Connect call processing. They represent the ATM Control Link (ACL) and Expansion Archangel Link (EAL).
- VBRnrt virtual circuits are also be used for ISDN channels between S8700 Multi-Connect PNs.
- Other VBRnrt virtual circuits may exist between A500 ports that are not associated with S8700 Multi-Connect PNs. A common use of VBRnrt circuits is multimedia and video-conferencing systems.

**Are talk paths being established between PNs?**

## Diagnostics

- Can you talk both ways on a set on one PN dialed from another PN, and vice versa?

**1** Enter **show switch circuit** on the A500 console. Figure 56, A500:show switch circuit screen, on page 198 shows the screen output.

**Figure 56: A500:show switch circuit screen**

```
A500:show switch circuit
 ____________________________________________________________
|    Input      |    Output     |        Connection          |
| port vpi  vci| port vpi  vci| type class  parameters       |
|______________|______________|____________________________|

  A1.1   0    5  Self   0    1  pp   UBR    ppd on
  A1.1   0   32  A1.2   0   32  pp   VBRnrt pcr=5729  /scr=5729  /mbs=17187
  A1.1   0   35  A1.2   0   35  pmp  CBR    pcr=173

  A1.2   0    5  Self   0    2  pp   UBR    ppd on
  A1.2   0   32  A1.1   0   32  pp   VBRnrt pcr=5729  /scr=5729  /mbs=17187
  A1.2   0   34  A1.1   0   34  pmp  CBR    pcr=173

  Self   0    1  A1.1   0    5  pp   UBR    ppd on
  Self   0    2  A1.2   0    5  pp   UBR    ppd on
_____________________________________________________________
```

— The pmp Constant Bit Rate (CBR) virtual circuits (VCs) between A500 port A1.1 (PPN) and A500 port A1.2 (PN) are used for talk paths between PNs.

— They are established when calls are first setup between PNs. Each virtual circuit represents one party of a complete multiparty talk path.

— The report above shows one complete talk path: one unidirectional point-to-multipoint virtual circuit from A1.1 to A1.2, and another from A1.2 to A1.1.

— These virtual circuits may persist beyond the duration of a phone call. The call-processing software saves virtual circuits for a few seconds after the end stations have hung up, in case the VC can be reused for another call between the same two PNs.

— In early version of the Release 2 A500 firmware, these connections incorrectly identified as `pmp UBR`.

— There may be other CBR virtual circuits between A500 ports that are not associated with S8700 Multi-Connect PNs. A common CBR application is circuit emulation, where T1, T3, etc. circuits are carried over ATM.

# Unusual ATM trouble conditions

There are a few failure modes in the S8700 Multi-Connect/A500 combination that are particularly difficult to diagnose. One example might be that you can't make a completely successful call, even though most indications from S8700 Multi-Connect and the A500 look pretty good. This section documents some hints and clues that may help diagnose the following failure modes:



## Incorrect PN Route or End System Identifier (A500)

### *Symptoms*

One-way talk paths from the PPN to a PN. You can hear tones from the PPN's end station to a PN's end station, but not vice versa. Since a signaling channel is a bidirectional VC established from the PPN to a PN, these can be routed correctly and come up just fine. However, a single call's talk path consists of two unidirectional VCs — one from the PPN to a PN (which is routed correctly) and another from the PN to the PPN (which cannot be routed).

### *Diagnostics*

1. At the A500 use the **show signaling routes** or **show signaling esi** command(s) as appropriate to check the ATM addresses.
2. Use **show signaling stats *port* q93b** on the PN's port, and look for cause code 3 (`No route to destination`).

### *Action*

Correct the ATM address translations in the A500.

## Swapped Routes, End System Identifiers, or Fiber between a PPN and a PN

### *Symptoms*

- An incorrectly connected PN TN230X does not complete board insertion.
- Dial tone is present for correctly connected PNs, but not for an affected PN's end stations.
- Calls cannot be made between the PPN and correctly connected PNs, because talk paths cannot be routed correctly.

### *Diagnostics*

The **show switch circuit table** command on the A500 shows VBR control channels from the A500 port intended for the incorrectly connected PN (but actually connected logically or physically to the PPN) that should not exist.

## Action

Correct the ATM addresses (or swap fibers) on the A500 between the incorrectly connected PPN and PN.

## Swapped Routes, End System Identifiers, or Fiber between two PNs

### *Symptoms*

- Every TN230X completes board insertion.
- The PPN cold starts both incorrectly connected PNs as usual.
- Both PNs log many `WRONG BOARD INSERTED` errors (use **list configuration all** or **display circuit-packs *carrier***), provided the PNs actually do have different boards configured in the same slots.
- Some end stations may work if they are connected to the correct board in the same slot on both PNs. Otherwise, the PPN's end stations have dial tone, while the PN's end stations do not.
- Every A500 diagnostic command looks good.

### *Diagnostics*

Check log for `WRONG BOARD INSERTED` errors (use **list configuration all** or **display circuit-packs *carrier***).

### *Action*

Correct the ATM addresses (or swap fibers) on the A500 between the incorrectly connected PNs.

## Swapped Routes, End System Identifiers, or Fiber between A- and B-side TN230Xs in a PN

### *Symptoms*

- The PPN establishes links to what it thinks is the active TN230X in the PN.
- As normal, it reboots this TN230X. When complete, it resets the PN. When this happens, the active (instead of the standby) TN230X reboots, dropping the links.
- To recover, the PPN re-establishes links to what it thinks is the active TN230X, and the cycle repeats indefinitely.

### *Diagnostics*

The **status pnc** command on the S8700 Multi-Connect SAT shows both the A and B side's `State of Health` field as `partially functional`.

### *Action*

Correct the ATM addresses (or swap fibers) on the A500 between the A and B side of the PN.

# Troubleshooting Multimedia Call Handling (MMCH)

## Expansion Services Module

An Expansion Services Module (ESM) provides T.120 data sharing capability on a MMCH multipoint H.320 video conference. Each conference participant must have endpoints administered and a personal computer with the H.320 video application installed. The S8700 Media Server system must have the expansion service module installed.

**Figure 57: Typical ESM connections**

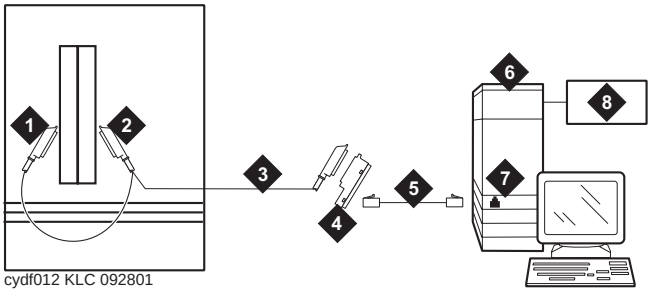



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Port B Y-cable connector to a TN787 Multimedia Interface (MMI) circuit pack | **5** | D8W cord connected to 356A adapter port 1 |
| **2** | Port A Y-cable connector to a TN2207 PRI circuit pack | **6** | Expansion Service Module (ESM) |
| **3** | 25-pair Y-cable | **7** | Port B on compatible primary rate interface (PRI) card |
| **4** | 356A adapter | | |

**CAUTION:**
The TN2207 circuit pack is the only pack allowing connection of an ESM to a S8700 Media Server system.

Before troubleshooting any problems associated with the MMCH, always be sure that the endpoint is operating correctly (audio, video, and data) by making point-to-point test calls. If possible, make the test calls over the network to test the connectivity and routing of network calls from the endpoint. This eliminates problems such as disconnected audio or video cables and network troubles.

## 64-kbps calls terminate, but far end receives 56-kbps indication

### *Description*

Some 2 x 64-kbps conferences on the S8700 Media Server MMCH are not established because of framing, audio, or video problems.

For calls that are routed in the network through an Avaya/LEC interface, the originating equipment may launch a 64-kbps call attempt, and the far end receives either a 56- or 64-kbps indication. If the far end receives a 64-kbps indication, the call may have used 56-kbps facilities. If so, the call may exhibit any of the following conditions:

- No handshaking in one direction or both (call disconnects after timeouts)
- Call connects, but audio or video is corrupted (audio noise or no video)
- Call succeeds without disruption (least likely, since one endpoint must realize that the call is using 56-kbps facilities)

If any of the above conditions occur, then 64-kbps calls from the site are blocked.

### *Solution*

Administer the conference for connection at 56 kbps.

## Calls terminate with no audio

### *Description*

To support endpoints that do not support Multipoint Command Conference (MCC), the MMCH changes its capability set and initiates a capability set exchange with the endpoint when the Selected Communications Mode (SCM) changes. If the endpoint does not follow the SCM audio mode, the MCU may include the endpoint as a secondary (audio only) endpoint. If the endpoint sends an unknown or unsupported audio mode, then the TN788B decoder port mutes the endpoint from the conference. The user may hear the conference but may not be heard by other conference parties.

### *Solution*

1. Use the Status Conference x screen and check the `Audio Mode` field for the current operating mode of the conference.
2. Another indication of the audio modes is in the “Incoming Mode Commands from Endpoint and Outgoing Commands from MMI” field on page 3 of the Status Conference x Endpoint y screen. Check the `Audio` fields under the Mode Commands/Communication Modes section of the screen.

## Some parties cannot be heard by others (audio subsetting)

### *Description*

Problems where varying subsets of the conference hear different things may have problems with the various summing resources/groups that are in use. Traditionally, these faults are caused by the server not cleaning up the connections properly. Isolation and diagnosis should focus on the VC resources in use by that conference.

### *Solution*

1. Use the **status conference** command to list the VC resources in use by this conference. Try a hot replacement of any VC boards in use (which refreshes the VC translations), and move every audio connection to a different VC port.
2. If the problem still exists, try dropping the conference and then bringing the conference back up again. Not only does this refresh VC translations, but uses different timeslots as well.
3. If the problem still exists, suspect a hardware problem. If practical, wait for the S8700 Media Server MMCH to be idle (no active conferences), and then check the circuit packs for active (amber) LEDs. If any of these are unexpected, such as on a VC board, try replacing the board and then bringing the conference up again.

## Calls terminate with no video

### *Description*

Generally, loss of video can be divided into two types. The first occurs when the MMCH switches to the endpoint, but nobody sees them. The receivers see either “black” video or a frozen image of the previous speaker, depending on the codec of the manufacturer. The type occurs when the MMCH does not switch to an endpoint.

### *Solution*

In the first type described above, wiring problems, power to the camera, or video encoder circuit pack problems in the codec are typical causes.

In the second type, no video from an endpoint typically occurs because it is not a valid video source. Check this on page 1 of the Status Conference x Endpoint y Vid screen under the Capability section. In this section, a “y” or “c” suggests that the endpoint has video. An “e” means ept has not declared any video capability in cap set, “n” is audio only, and “blank” means audio add-on.

Also check page 1 of the Status Conference x Endpoint y Vs screen for indication of the video state for the endpoint values.

## Calls terminate correctly but are unstable

A number of conditions will lead to some or all endpoints having stability problems during the course of a conference. A lack of stability from an endpoint is noticeable by a lack of a video switching while the party is the only talker or excessive disconnects from that endpoint.

### *Synchronization*

Generally, the most common problem is a mismatch in synchronization sources between the endpoint and the S8700 Media Server MMCH. This typically causes low-level (Px64) handshake problems that can trigger the endpoint/MMCH to disconnect the call. The MCCH's timers are set to sufficiently high values so that, normally, the endpoint will timeout and disconnect first. If installed in a customer network, it is a good idea to perform an audit of the path synchronization is being supplied. If there are different clock sources between endpoints and the S8700 Media Server MMCH, some problems are sure to occur. The severity of these problems can range from a handshake failure every few seconds to one per day. Depending on the type of endpoint, this can cause the endpoint to disconnect or just freeze video until the main problem is resolved.

Specifically, PictureTel System 4000 endpoints seem to be the most sensitive to instability. The Avaya Vistium disconnects fairly infrequently. The CLI Rembrandt II VP freezes video and waits for framing to be recovered.

### *Network configuration concerns with synchronization*

When auditing a network for synchronization, avoid unnecessary hops. Thus, a switch providing star-configuration synchronization is preferred over a daisy-chain configuration. Additionally, if there are S8700 Media Server systems that have PNs, synchronization should be provided to subnodes from the same PN through which the system receives its synchronization. Passing synchronization through a a system's EI:

- Adds an unnecessary hop to the path
- Creates another potential point of failure

### *Expansion Interface duplication*

If a customer's network uses PNs with duplicated EIs, scheduled switching of the EI links should be disabled on the PBX by using **change system-parameters maintenance**. When scheduled maintenance runs and switches the links, there is a brief corruption of the data path. If endpoints have active calls when the switch occurs, this corruption of the data path causes Px64 handshake problems that lead to the endpoints losing video source status and sometimes disconnecting as described above. Disabling the EI switching is in the customer's best interest to prevent the disruption of the Px64 data stream. The customer gets the same level of alarm indications and maintenance on the EI links, regardless of the status of scheduled switching.

### *PRI D-channel backup*

A somewhat unlikely source of call-stability problems can be incorrectly translated PRI D-channel backup between two non-MCU systems. As an example:

- System A's DS1 1A10 is assigned as the ***primary*** source
- System B's corresponding DS1 is assigned as the ***secondary*** source

Then (when scheduled maintenance runs on either system with its backup D channel ***active***), an audit disconnects some calls using the link. This problem is corrected by assigning matching primary/secondary D channels for the two systems.

### *Processor duplication in the system*

Do not enable the PI link switch during scheduled maintenance. This can cause link-stability problems on the Accunet Bandwidth Controller (ABC).

## Voice-activated switching problems

Voice-activated switching on the S8700 Media Server Multimedia Call Handler (MMCH) does not follow the loudest talker. The MMCH queues every speaking party and selects a new video broadcaster (the second-oldest speaking party) when the oldest speaking party has stopped talking. The new broadcaster will see the last speaker as its video. The system can also "learn" about the noise coming from an endpoint to help prevent false switches, adapting both to noise level and repetitive sounds such as a fan. This adaptation occurs over approximately 10 seconds.

## No switching, full-motion video

If a room is excessively noisy:

- The S8700 Media Server MMCH may receive sufficient audio signal to conclude that there is a speaker present. Use the Status Conference x screen to determine whether the MMCH thinks an endpoint is talking. The MMCH sets the `Ts` field to `t` for each endpoint if there is voice energy detected. This endpoint may have to mute when nobody at the site is speaking to allow the conference to proceed normally.
- Remind the customer that it may be necessary to mute if a side conversation is going on in the background, just as one would do in an audio conference.
- If the system does not switch broadcasters even after the current broadcaster has muted, check the conference administration using the **display conference *X*** command to ensure that the conference is in voice-activated mode. Also verify that parties who were speaking are valid video sources as described in Calls terminate with no video on page 203.

The See-Me feature (MCV) can also cause VAS to "lock-up." An endpoint can activate MCV to force their site to become the broadcaster. If they do not disable the feature when finished, the system remains in this mode indefinitely. The **status conference *X*** command shows that MCV is in effect by displaying `av` in the Video Status (Vs) column. Page 3 of the Status Conference X Endpoint Y screen also has a `Broadcaster` field that indicates MCV is in effect with (SEE-ME) as the broadcaster.

The same scenario can occur in a CHAIR or UCC-controlled conference with a designated broadcaster. In this situation, the CHAIR/UCC has not released the designated broadcaster and returned to VAS mode. If there is a UCC-designated broadcaster, **status conference X** indicates a Video Status of `u`. Also, for UCC rollcall the return video may appear to be stuck. Check the Video Status for an "`R`," indicating rollcall.

If none of the previous examples appears to be the cause and if the room was quiet, every speaker is a valid video source, the conference is voice-activated, and the speaker can be heard, then escalate the problem.

## Video never switches to a particular party

### *Description*

Verify that the endpoint is a valid video source as described in Calls terminate with no video on page 203. If it is, then the audio from the endpoint may not have sufficient voice signal for the hardware to determine that the parties at the endpoint are speaking. Check the `Talk` field on page three of the Status Conference X Endpoint Y screen to see if the `talking bit` is `y`. Next, check the audio by standing adjacent to the microphone and speaking at a normal level.

### *Solution*

If the audio is not muffled:

1. Use the **status conference** command to determine which port on the TN788B (VC board) is connected to this endpoint.
2. Check the VC (TN788B) board using the **test board *xxyy* long** command.
3. Drop the call.
4. Find another available port, then:
   a. Busyout the port to which the endpoint was connected.
   b. Make another call to the same conference. If the problem corrects itself, then the previous port may be bad. If there are other VC boards with sufficient available ports to replace calls on the current VC, then pull the board that has the bad endpoint on it (the **status conference** command displays the encoder port associated with the call). The system will automatically reestablish the VC connections without dropping the call. If this fixes the problem, then replace the board, as it has at least one bad port. Reseating the board may temporarily fix the problem due to the hard reset done to the board.

## Audio echo

Echo in conference calls, particularly those with large delay characteristics, is totally disruptive. When Voice Activated Switching is taken into account, the effects are disastrous. Various arrangements of the microphone(s) and room speaker(s) might be needed. Table 63, Audio echo troubleshooting, on page 206 details two common audio echo problems and suggested actions to resolve them.

**Table 63: Audio echo troubleshooting**

| Situation | Problem | Action |
|---|---|---|
| For some Avaya Vistium endpoints, an external speaker may be attached or was attached when the system was last rebooted | Endpoint causes audio echo throughout the conference | Isolate the offending endpoint by asking each endpoint to mute, one at a time, until the echo disappears. |
| Input from an endpoint is too near an endpoint's speakers | Acoustic echo is created | Move the microphone away from the speakers. |

Normally, if any microphone in the room is moved relative to the speakers, that site will cause echo until the echo canceller in the codec retrains itself. Some will require a manual reset.

If a PictureTel keypad is configured with external microphones connected to the keypad, then the internal microphone and external microphone(s) "sing" to each other if the "ext mic" bat switch is set to "int mic" on the back of the keypad. In this configuration, VAS locked on that site, and the acoustic "singing" was inaudible.

## Rate adaptation

Because of a lack of a clear explanation in standards, sometimes endpoints do not work well with each other and the S8700 Media Server MMCH. The MMCH will only allow a conference to downgrade from 64- to 56-kbps operation on conferences that have the `Rate Adaptation` flag set to `y`.

When a downgrade does occur, information on the Status Conference screen indicates the success or failure of the 64-kbps endpoints that are participants to properly rate adapt to 56 kbps. As a general indication that the conference has rate adapted, the `Conference Transfer Rate` and `Effective Transfer Rate` fields show initial and current transfer rates, respectively.

- For each 64-kbps endpoint, the column that indicates `Rate Adapt` shows an `n` if the endpoint did not follow the procedures as specified by the H.221.
- If an endpoint shows `y`, it did successfully rate adapt.
- If an endpoint shows `c`, it joined the conference at 56 kbps.

Once the conference rate adapts, the endpoints that do not properly follow suit, will become audio-only endpoints. A conference will not rate adapt from 56 back to 64 kbps until every endpoint disconnects from the conference and it idles.

The PictureTel 1000 Release 1.1C, PictureTel 6.01 software, and the Vistium 2.0 software successfully rate adapt with the MCU. External rate adaptation techniques used by VTEL and CLI are known to cause problems with the endpoint when used with this feature.

### Endpoint or I-MUX in loopback mode

Some endpoints have a loopback enable feature. This makes MMCH data loopback at the MMCH when a connection is in progress. The loopback can be enabled prior to or during a connection.

The MMCH does not detect the loop and continues to VAS. In most scenarios, the switch occurs, but within a few seconds, the broadcaster's return video becomes its own image. Once the broadcaster stops speaking, the system "false" switches to an apparently random port that was not speaking.

## Troubleshooting ISDN-PRI

The following flow chart defines a layered approach when troubleshooting ISDN-PRI problems. Since a problem at a lower layer affects upper layers, layers are investigated from low to high. In the flowchart, the DS1 facility is layer 1, the ISDN-PRI D channel is layer 2 (**S8100**: TN765 Processor Interface), and the ISDN trunks are layer 3. Transient problems are diagnosed on Page 2 of the flowchart. For problems with PRI endpoints (wideband), see the following section.

**Figure 58: Troubleshooting ISDN-PRI (Page 1 of 2)**

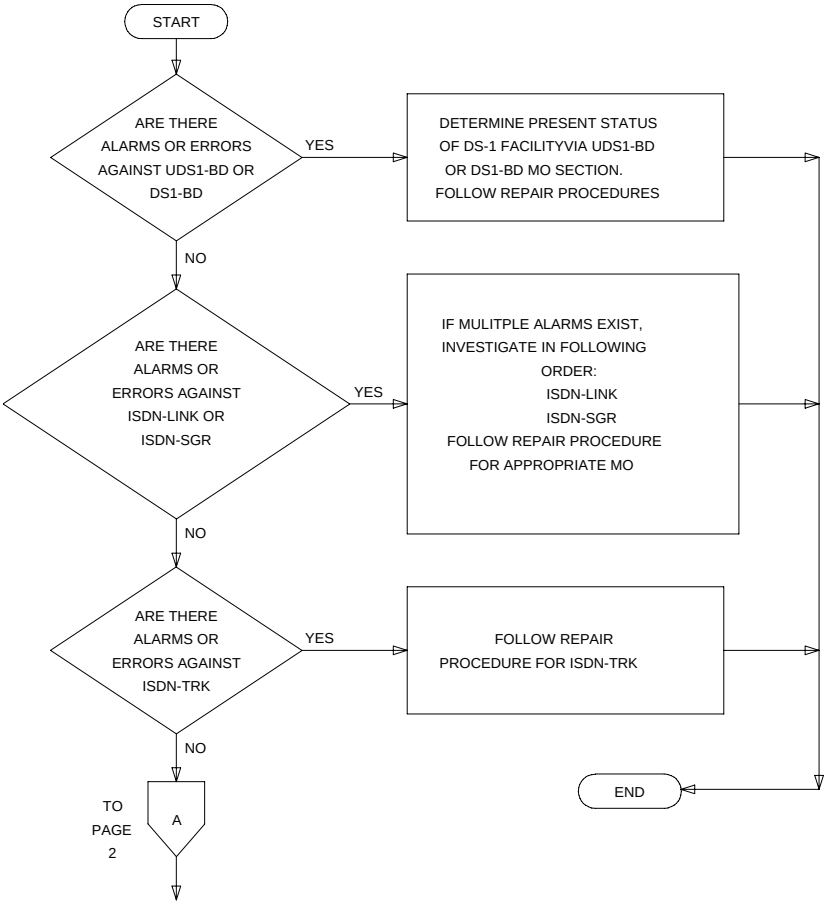
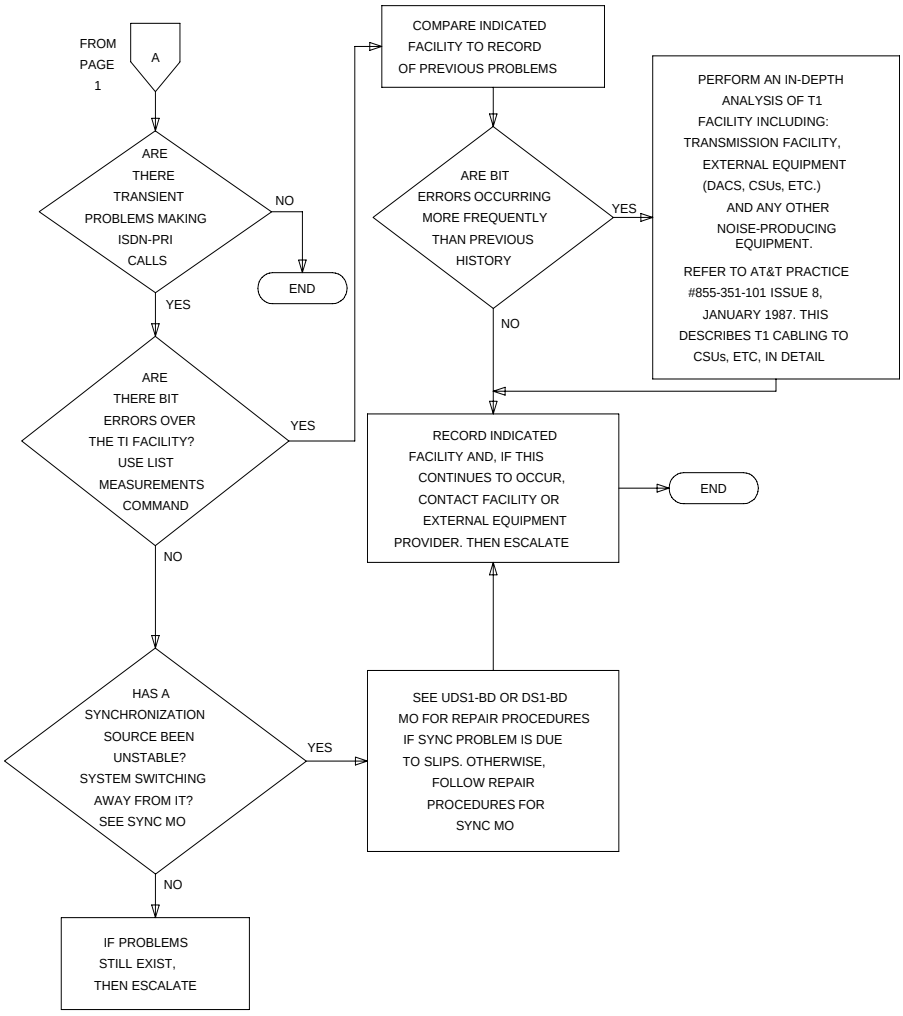


**Figure 59: Troubleshooting ISDN-PRI (Page 2 of 2)**




# Troubleshooting ISDN-PRI endpoints (wideband)

The following flow chart describes a layered approach for troubleshooting problems with an ISDN-PRI endpoint. Because problems at lower layers affect upper layers, layers are investigated from low to high. In this procedure, the:

- DS1 facility is layer 1
- TN2312AP IPSI circuit pack's Packet Interface circuit is layer 2 (**S8100**: TN765 Processor Interface is layer 2)
- PRI endpoint's ports are layer 3 (**S8100**: ISDN trunks are layer 3)

This troubleshooting procedure is limited to diagnosing faults between the switch and either the ISDN-PRI's:

- Line-side terminal adapter
- Endpoint equipment

Problems encountered on the network side of a wideband connection or problems with end-to-end equipment compatibility are beyond the scope of this section.

| | | |
|---|---|---|
| START | | |
| Are there alarms or errors against any of the following maintenance objects (MOs): UDS1-BD, PKT-INT, SYS-LINK, ISDN-LNK, ISDN-SGR, PE-BCHL<br>↓ NO | YES<br>→ | Resolve those alarms or errors in the order listed at left by following procedures for the appropriate MO in *Maintenance Alarms Reference (555-245-102)*. |
| Check the status of the endpoint equipment or terminal adaptor. (Do this at the endpoint, not at the G3-MT.) ↓ | | |
| Does the adaptor or endpoint indicate problems?<br>↓ NO | YES<br>→ | Follow repair procedures recommended by the provider of the terminal adapter or endpoint equipment. |
| Check administration at the endpoint and on the switch (for example, port boundary width). Are they inconsistent?<br>↓ NO | YES<br>→ | Correct the administration so that both ends match. |
| Does every call fail, or are the failures transient?<br>↓ Transient Failures | Always Fails<br>→ | Check the health of the application equipment (for example, the video codec) and that of the S8700 Media Server network. If constant failures persist, follow normal escalation procedures. |
| Use **list measurements ds1** to check for bit errors over the DS1 interface between the switch and the terminal adapter or endpoint equipment.<br>↓ No bit errors | Bit Errors<br>→ | Perform an in-depth analysis of the DS1 interface including premises distribution wiring, endpoint equipment, and any other possible source of noise. If the problem cannot be isolated, follow normal escalation procedures. |
| Check for alarms and errors against SYNC. Has a synchronization source been unstable, or has the system switched synch sources?<br>↓ NO | YES<br>→ | Follow procedures described in SYNC in *Maintenance Alarms Reference (555-245-102)*. |
| Follow normal escalation procedures. | | |

### S8100

On the S8100, Figure 60, Processing of PRI endpoint problems (page 1 of 2), on page 211 and Figure 61, Processing of PRI endpoint problems (page 1 of 2), on page 212 show the processing of PRI endpoint problems.

**Figure 60: Processing of PRI endpoint problems (page 1 of 2)**

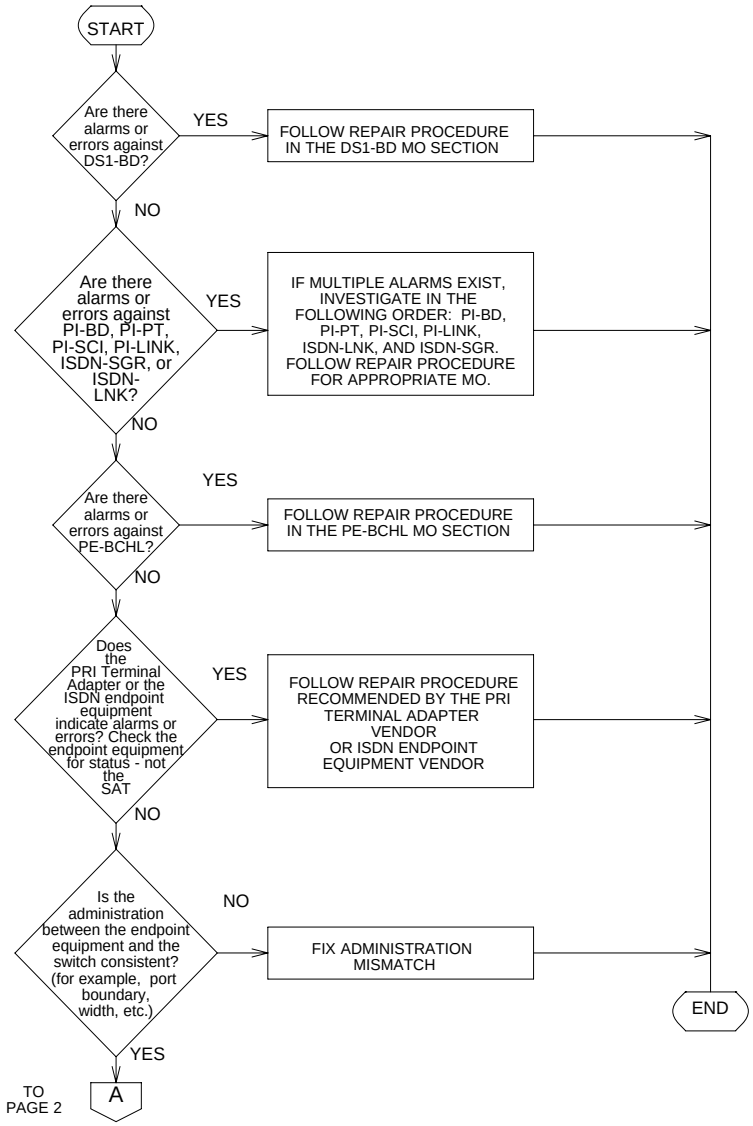
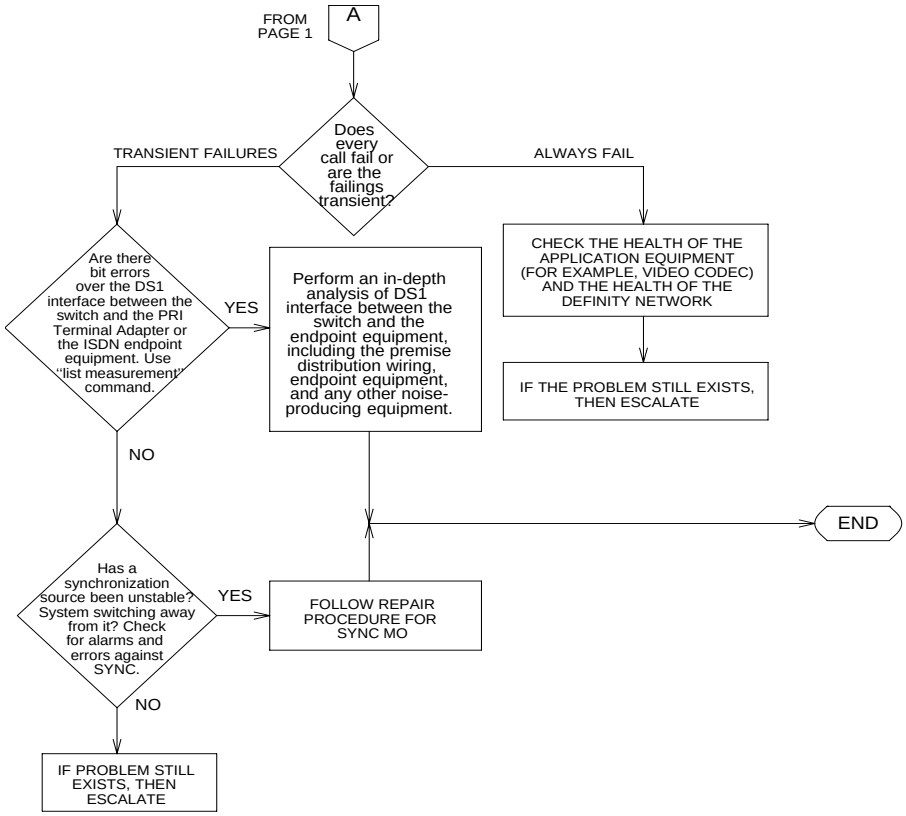


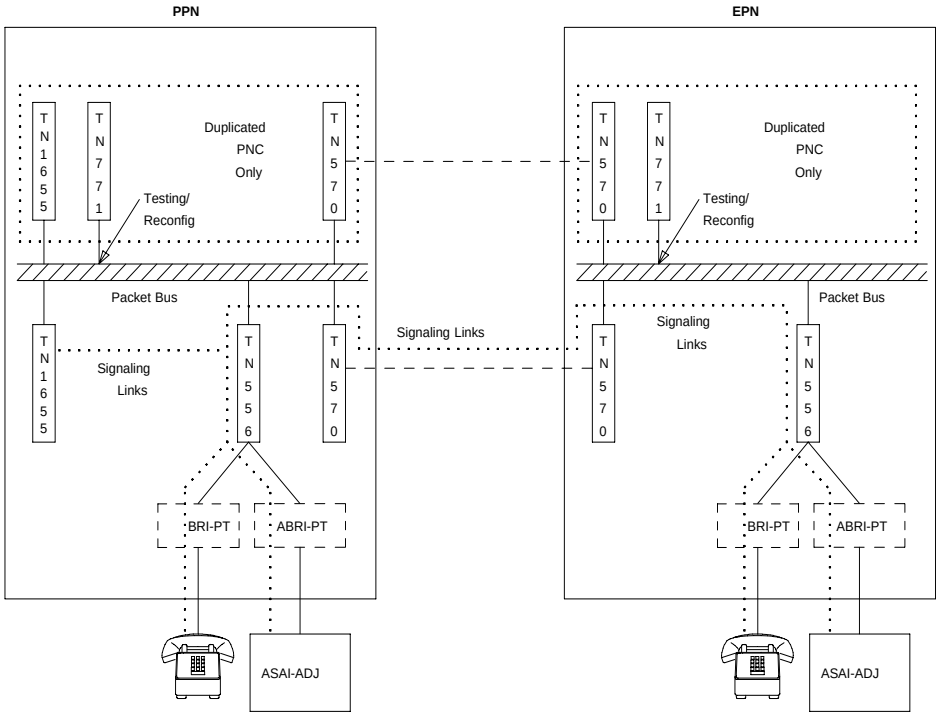
**Figure 61: Processing of PRI endpoint problems (page 1 of 2)**




# Troubleshooting ISDN-BRI / ASAI

Troubleshooting ISDN-BRI/ASAI problems can be a complex and involved procedure. The reason for this is that ISDN-BRI devices communicate with the server over the packet bus, as opposed to the TDM bus. Therefore, it is possible for another component's fault (related to the packet bus) to cause problems with ISDN-BRI devices. Figure 62, ISDN-BRI/packet-bus connectivity, on page 213 shows the connectivity of the packet bus as it applies to ISDN-BRI signaling.

**Figure 62: ISDN-BRI/packet-bus connectivity**




The flowchart in Figure 63, Troubleshooting ISDN-BRI problems (Page 1 of 2), on page 214 describes the steps needed to isolate and resolve an ISDN-BRI problem. The order of examining maintenance objects (MOs) can be determined by assessing how wide-spread the failure is. For example, since every ISDN-BRI device in the PN or IPSI-connected PN communicates with the TN2312AP IPSI circuit pack's Packet Interface circuit, its MO should be examined early in the sequence. On the other hand, a failure of a PN's TN570 EI circuit pack may cause an ISDN-BRI failure in one PN, but not in another.

> **NOTE:**
> If the flowchart query "Is the problem affecting MOs on multiple BRI-BD circuit packs?" is reached and the PN in question has only one ISDN-BRI circuit pack, then assume that the answer is "Yes," and follow the repair procedure for PKT-BUS.

When directed by the flowchart to refer to the maintenance documentation for a specific MO, keep in mind that the repair procedure for that MO may refer you to another MO's repair procedure. The flowchart tries to coordinate these activities so that a logical flow is maintained if the ISDN-BRI problems are not resolved with the first set of repair procedures.

These following **status** commands may also be useful when diagnosing ISDN-BRI problems:

- status port-network
- status packet-interface
- status bri-port
- status station
- status data-module

**Figure 63: Troubleshooting ISDN-BRI problems (Page 1 of 2)**

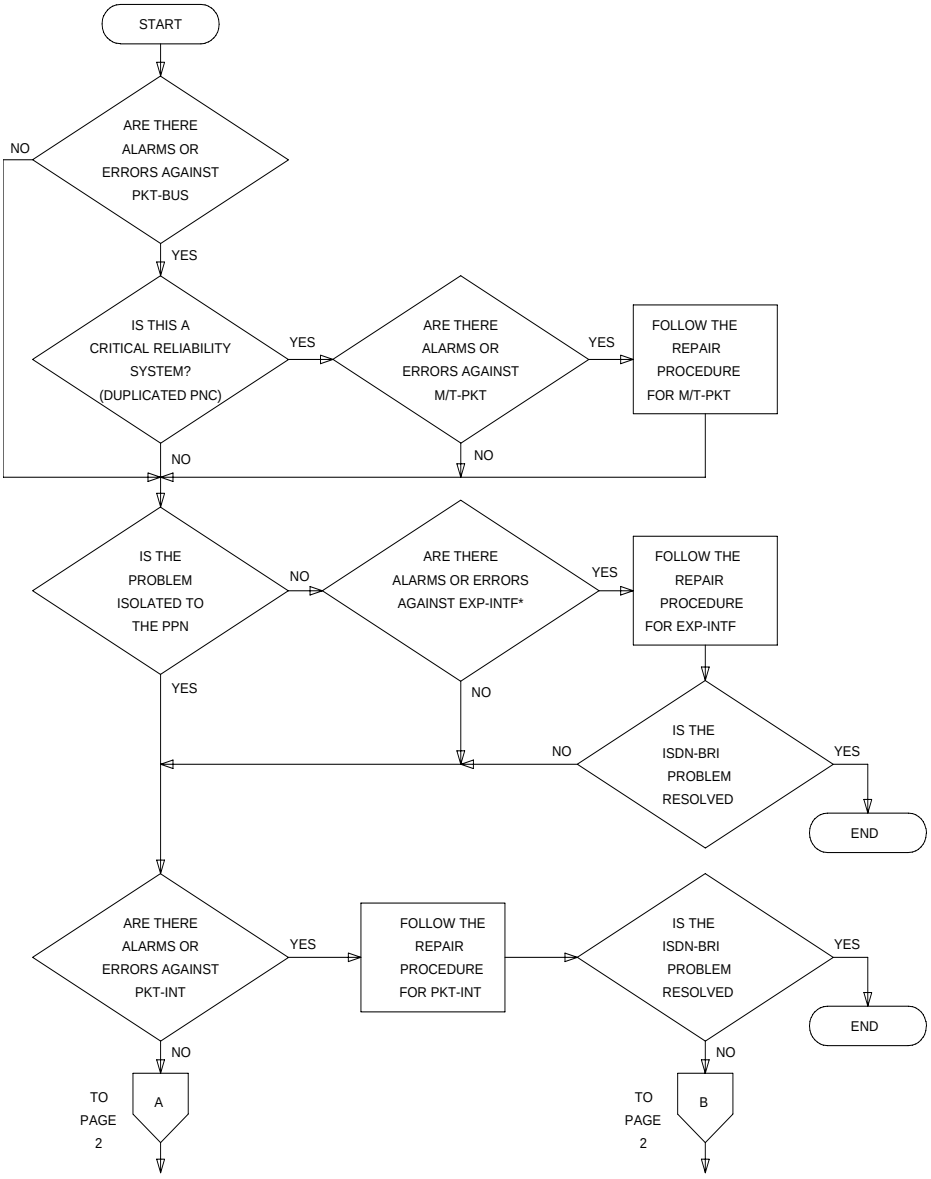
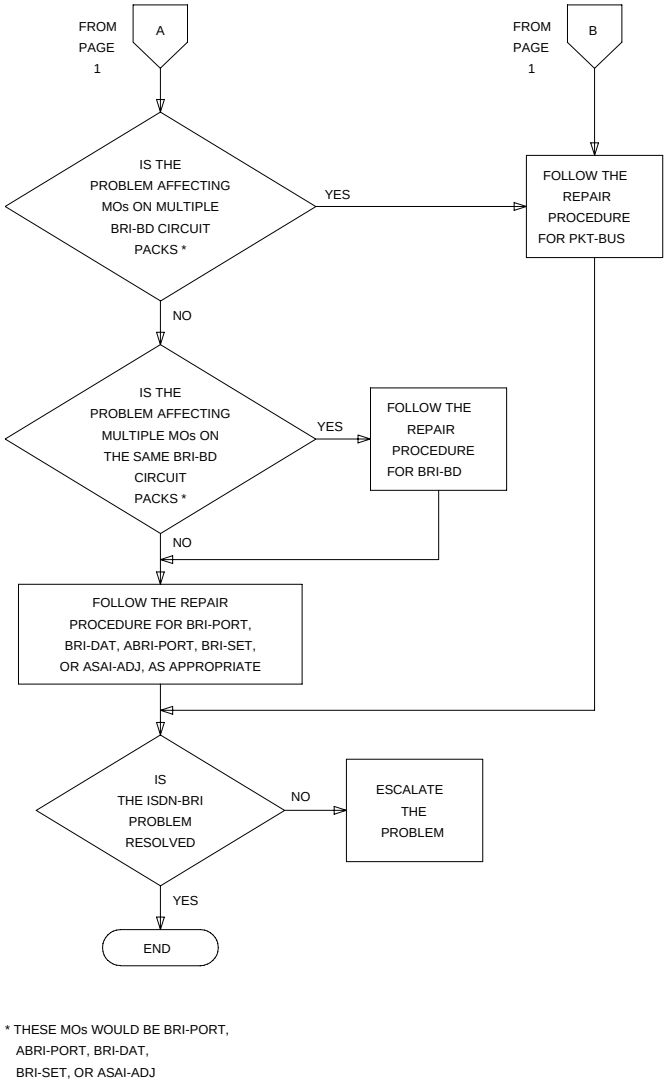


**Figure 64: Troubleshooting ISDN-BRI problems (Page 2 of 2)**




# Troubleshooting ISDN-PRI test calls

An ISDN-PRI test call is placed across an ISDN-PRI user-network interface to a previously designated number in order to test ISDN capabilities of the switch, the trunk and the far end. An ISDN-PRI test call is also a maintenance procedure concerned with the identification and verification ISDN-PRI user-network interface problems. The ISDN-PRI test call can access ISDN-PRI trunks only.

An ISDN-PRI test call can be placed only if the circuit translates to an ISDN-PRI trunk. An ISDN-PRI test call can be originated through either the *synchronous* or the *asynchronous* method. Each method is described in the following sections.

**NOTE:**
Before attempting to make an ISDN-PRI test call to the public network (the far end), make sure that test call service is provisioned by the network. The user must subscribe to Test Type 108 service and have the correct far-end test call number administered on the Trunk Group screen for the call to be allowed.

## Synchronous method

One command is used in this method to start, stop, and query an ISDN-PRI test call. In the synchronous method, an outgoing ISDN-PRI test call may be part of one of the following *long* test sequences entered at the terminal:

- test trunk *grp/mbr* long [*repeat#*]
- test port *UUCSSpp* long [*repeat#*]
- test board *UUCSS* long [*repeat#*]

The **long** qualifier must be entered in the above commands in order for the ISDN test call to run. The repeat number (#) can be any number from 1 through 99 (default = 1).

The following information is displayed in response to the above commands:

- Port: The port address (UUCSSpp) is the PN's number, carrier designation, slot, and circuit of the maintenance object (MO) under test.
- Maintenance Name: The type of MO tested.
- Test Number: The actual test that was run.
- Test Results: Indicates whether the test passes, fails, or aborts.
- Error Code: Additional information about the results of the test. For details, see ISDN-TRK (DS1 ISDN Trunk).

## Asynchronous method

The asynchronous method requires a Maintenance/Test circuit pack to be present in the system. In this method, 4 commands are used to start, stop, list, and query an outgoing ISDN-PRI test call:

| | |
|---|---|
| Start: | test isdn-testcall *grp/mbr* [*minutes*] |
| Stop: | clear isdn-testcall *grp/mbr* |
| List: | list isdn-testcall |
| Query: | status isdn-testcall *grp/mbr* |

Before placing an outgoing ISDN-PRI test call, verify that the feature access code has been administered on the System Features screen, and that the far-end test line number and TestCall Bearer Capability Class (BCC) have been administered on the Trunk Group screen. If the ISDN-PRI trunk is cbc (call by call) service type, the `Testcall Service` field on the Trunk Group screen must also be administered.

To initiate an outgoing ISDN-PRI test call with the asynchronous method, issue the start command listed above, which enables you to specify a specific the trunk on which to originate the ISDN-PRI test call. An optional qualifier can be used that specifies in minutes (1 to 120) the duration of the test call. If no duration is specified, the default is either 8.4 or 9.6 seconds.

Figure 65, Test ISDN-TestCall Response, on page 217 shows a typical response to the **test isdn-testcall** command:

**Figure 65: Test ISDN-TestCall Response**

```
test isdn-testcall

Port    Maintenance Name   Test Number   Test Result  Error Code
1B1501  ISDN-TRK              258           PASS
```

The displayed fields have the following meanings:

| | |
|---|---|
| `Port` | The port address (UUCSSpp) is the port network's number, carrier designation, slot, and circuit of the maintenance object (MO) under test. |
| `Maint. Name` | The type of MO tested. |
| `Test Number` | The actual test that was run. |
| `Test Results` | Indicates whether the test passes, fails, or aborts. |
| `Error Code` | Additional information about the results of the test. See the ISDN-TRK section in *Maintenance Alarms Reference (555-245-102)* for details. |

The functions of the **clear**, **list**, and **status** commands associated with the ISDN Testcall are summarized in Troubleshooting the outgoing ISDN-testcall command on page 218.

- **clear isdn-testcall**: Enables you to cancel an in-progress ISDN-PRI test call and allow another test call to start.
- **list isdn-testcall**: Enables you to list every ISDN-PRI trunk in use for an ISDN-PRI test call in the system.
- **status isdn-testcall**: Enables you to check the progress of an outgoing test call. When an outgoing ISDN-PRI test call completes in a specific PN, another ISDN-PRI trunk from the same PN is available for testing (regardless of whether the **status** information has been displayed).

# Troubleshooting the outgoing ISDN-testcall command

If the `TestCall BCC` field appears on the Trunk Group screen, ensure that the `TestCall BCC` field indicates the correct BCC for the service provisioned on the ISDN-PRI trunk. The `TestCall BCC` values are defined as follows:

| | |
|---|---|
| `0` | Voice |
| `1` | Digital Communications Protocol Mode 1 |
| `2` | Mode 2 Asynchronous |
| `3` | Mode 3 Circuit |
| `4` | Digital Communications Protocol Mode 0 (usually the default). |

If the ISDN-PRI trunk is of type `cbc` make sure the `TestCall Service` field on the Trunk Group screen indicates the correct service so that a network facility message can be sent across the ISDN-PRI network.

If the outgoing ISDN-PRI test call keeps aborting, make sure that the far-end device can handle DCP Mode 0 or DCP Mode 1.

**NOTE:**
Before attempting to make an ISDN-PRI test call to the public network (that is, the network is the far end), make sure that test call service is provisioned by the network. The user must subscribe to Test Type 108 service and have the correct far-end test call number administered on the Trunk Group screen for the call to be allowed.

# 7 Packet and serial bus maintenance

The topics covered in this chapter include:



## Isolating and repairing packet-bus faults

**NOTE:**
This material *does not* apply to **S8100**; see S8100 packet bus fault isolation and repair on page 245 for fault isolation and repair procedures for **S8100**.

The following procedures provide a means of isolating and correcting faults on both the packet bus and the various maintenance objects (MOs) that use the packet bus. The packet bus is shared by every circuit pack that communicates on it, and a fault on one of those circuit packs can disrupt communications over the packet bus. Furthermore, a circuit pack that does not use the packet bus can also cause service disruptions by impinging on the backplane or otherwise modifying the configuration of the bus. For these reasons, isolating the cause of a packet-bus problem can be complicated. This discussion provides a flowchart and describes the tools and procedures used to isolate and correct packet-bus faults.

The following sections provide background information and troubleshooting procedures. The Packet-Bus Fault Isolation flowchart is intended to be the normal starting point for isolating and resolving packet-bus problems. Before using it, you should familiarize yourself with packet-bus maintenance by reading the introductory sections.

- Remote versus on-site maintenance on page 220 discusses the strategy and the requirements for performing remote maintenance and on-site maintenance for the packet bus.
- Tools for packet bus fault isolation and correction on page 220 discusses the tools that are needed to isolate and correct packet-bus faults.
- What is the packet bus? on page 220 describes the packet bus, its use in G3r, and the types of faults that can occur on the packet bus. A diagram shows the physical and logical connections between circuit packs connected to the packet bus.
- Circuit packs that use the packet bus on page 222 describes the various circuit packs, ports, and endpoints that use the packet bus. This section discusses how these MOs interact, how a fault in one MO can affect another, and failure symptoms of these MOs.
- Packet bus maintenance on page 224 describes the strategy of maintenance software for packet bus. This section discusses similarities and differences between the packet bus and the TDM bus. An overview of the Fault Isolation and Correction Procedures is also presented.
- Maintenance/Test circuit pack (TN771D) on page 226 discusses the use of the Maintenance/Test circuit pack in both packet-bus fault isolation and other switch maintenance. The stand-alone mode of the Maintenance/Test circuit pack, which is used to perform on-site packet-bus fault isolation and correction, is discussed in detail.

- Packet bus fault isolation flowchart on page 234 is the starting point for the troubleshooting process. It is used to determine whether a failure of service is caused by the packet bus itself or by another MO on the packet bus.
- Correcting packet-bus faults on page 238 presents the procedures required to correct either a problem with the packet bus itself or one that is caused by a circuit pack connected to the packet bus.

## Remote versus on-site maintenance

Most packet-bus fault isolation and repair procedures require a technician to be on-site. This is because packet-bus problems are caused by a hardware failure of either the packet bus itself or a circuit pack that is connected to it. Initial diagnoses can be made using the Packet-Bus Fault Isolation flowchart, but the Maintenance/Test Stand-Alone Mode and Packet-Bus Fault Correction procedures require an on-site technician. These procedures are presented with this requirement in mind.

The flowchart refers to the repair procedures for various MOs. When a decision point is reached, a remotely located technician can refer to the appropriate section and attempt to resolve any fault conditions. Some procedures require on-site repair action. Keep in mind that failure of an MO appearing early in the flowchart can cause alarms with MOs that appear later in the flowchart. Multiple dispatches can be prevented by remotely checking subsequent stages on the flowchart and preparing the on-site technician for replacement of several components, if necessary.

The Maintenance/Test packet-bus port, described below, provides status information that is accessed with the **status port-network *P*** command and the PKT-BUS test sequence. The Maintenance/Test circuit pack may or may not be present at a customer site, depending on the configuration of the switch. If a Maintenance/Test circuit pack is absent, one must be taken to the site for diagnosing packet-bus problems.

### Tools for packet bus fault isolation and correction

The following tools may be required on-site to perform packet-bus fault isolation and correction.

- TN771D Maintenance/Test circuit pack for use in stand-alone mode, and the connectors and cables necessary to install it (see M/T-BD (Maintenance/Test Circuit Pack)).
- A replacement for the TN771D Maintenance/Test circuit pack in the system may be needed. See Entering and exiting stand-alone mode on page 229.
- A backplane pin-replacement kit may be required (see Correcting packet-bus faults on page 238). If the kit is not available, replacement of a carrier may be required.

## What is the packet bus?

The packet bus is a set of 24 leads in the backplane of each PN. Twenty of these leads are data leads, three are control leads, and one lead is a spare. This distinction is important only for understanding why some circuit packs can detect only certain faults; the distinction does not affect fault isolation and repair. Each PN has its own packet bus, and there is one Packet Bus MO (PKT-BUS) for each PN. Unlike the TDM bus, the packet bus is not duplicated. However, it has several spare leads and, in a critical-reliability system (duplicated PNC), these spare leads are used to recover from some packet-bus faults.

The packet bus carries various types of information:

- Signaling and data traffic destined for other port networks and/or Center Stage Switches (CSSs) through the TN570 Expansion Interface circuit pack access.
- ISDN-BRI signaling information for ISDN-BRI stations, data modules and ASAI adjunct connections. The TN556 ISDN-BRI circuit pack provides packet-bus access for these connections.
- ISDN-PRI signaling information carried in the D channels of ISDN-PRI facilities connected to the switch. The TN464F Universal DS1 circuit pack provides packet-bus access for these connections.

A server's interface to a PN's packet bus is by way of an Ethernet link to the PN's TN2312AP IPSI circuit pack, through the IPSI's Packet Interface circuit, and to the packet bus. When servers are duplicated, there are two IPSIs in each PN. The TN771D Maintenance/Test circuit pack provides packet-bus maintenance testing and reconfiguration capabilities. The circuit packs mentioned here are discussed in more detail in Circuit packs that use the packet bus on page 222.

## Packet-Bus faults

Two types of packet-bus faults can occur:

**Shorts** A short occurs when different leads on the packet bus become electrically connected to each other. This can occur due to failures of circuit packs, cables between carriers, TDM/LAN terminators, or bent pins on the backplane. A fault occurring during normal operation is usually caused by a circuit pack. A fault that occurs while moving circuit packs or otherwise modifying the switch is usually due to bent pins on the backplane.

**Opens** An open occurs when there is a break on the packet bus such that the electrical path to the termination resistors is interrupted. Usually, this break is caused by a failed TDM/LAN cable or terminator. A less likely possibility is a failure in the backplane of a carrier.

Shorts are far more common than opens since they can be caused by incorrect insertion of a circuit pack. It is possible for a circuit pack to cause a packet-bus fault, but still operate trouble-free itself. For example, the insertion of a TDM-only circuit pack such as a TN754 digital line could bend the packet-bus pins on the backplane but remain unaffected, since it does not communicate over the packet bus.

Packet-bus faults do not necessarily cause service interruptions, but shorts on it usually do. Depending on which leads are defective, the system may recover and continue to communicate. While this recovery can provide uninterrupted service, it also makes isolating a fault more difficult. The Maintenance/Test circuit pack enables the detection and, in some cases, correction of packet-bus faults.

## Packet bus connectivity

Various maintenance objects communicate on the packet bus (see the next section). For more details, use the following links for the following MOs:

- TN2312AP IP-SVR (IP Server Interface)
- PKT-INT (Packet Interface)
- TN570 EXP-INTF (Expansion Interface Circuit Pack)

- TN556 ISDN-BRI:
  - BRI-BD/LGATE-BD (ISDN-BRI Line Circuit Pack)
  - BRI-PORT (ISDN-BRI Port) ABRI-PORT (ASAI ISDN-BRI Port)
  - BRI-SET, BRI-DAT, Various Adjuncts
- TN464F Universal DS1:
  - UDS1-BD (UDS1 Interface Circuit Pack)
  - ISDN-PLK (ISDN-PRI Signaling Link Port)
- TN771D Maintenance/Test:
  - M/T-BD (Maintenance/Test Circuit Pack)
  - M/T-DIG (Maintenance/Test Digital Port)
  - M/T-PKT (Maintenance/Test Packet Bus Port)

## Circuit packs that use the packet bus

This section describes the circuit packs that use the packet bus and the mutual effects of circuit-pack and bus failures.

Seven circuit packs use the packet bus: The MOs associated with each circuit pack are listed in brackets:

- **TN2312AP IP Server Interface** [PKT-INT] provides a server's Ethernet interface to a PN's packet bus. All traffic on the packet bus passes through the TN2312AP IPSI circuit pack's Packet Interface circuit. This circuit can detect some control-lead and many data-lead failures by checking for parity errors on received data.
- **TN570 Expansion Interface** [EXP-INTF] connects the PNs in the system. All packet traffic between PNs passes through a pair of TN570s (one in each PN). The EI can detect some control-lead and many data-lead failures by way of parity errors on received data.
- **TN556, TN2198, or TN2208 ISDN-BRI** [BRI-BD, BRI-PORT, ABRI-PORT, BRI-SET, BRI-DAT, ASAI-ADJ] carries signaling information for ISDN-BRI station sets and data modules, as well as signaling information and ASAI messages between the server and an ASAI adjunct. Depending upon the configuration, an ISDN-BRI circuit pack has the same fault-detection capabilities as a TN570 EI circuit pack can detect some control-lead and many data-lead failures by way of parity errors on received data.
- **TN464F Universal DS1 circuit pack** [UDS1-BD, ISDN-LNK] supports ISDN-PRI communications over an attached DS1 facility. It transports D-channel signaling information over the packet bus, and B-channel data over the TDM bus. Depending upon the configuration, the universal DS1 circuit pack has the same fault-detection capabilities as a TN570 EI circuit pack can detect some control-lead and many data-lead failures by way of parity errors on received data.
- **TN771D Maintenance/Test circuit pack** [M/T-BD, M/T-DIG, M/T-PKT, M/T-ANL] is the workhorse and a critical tool of packet-bus maintenance. This circuit pack can detect every packet-bus fault in the PN where it resides. In a critical-reliability system (duplicated PNC), this circuit pack enables the reconfiguring of the packet bus around a small number of failed leads. The TN771D circuit pack provides a stand-alone mode (one not involving indirect communication with the server, through the IPSI) for inspecting packet-bus faults.

**NOTE:**
Every Maintenance/Test circuit pack must be of vintage TN771D or later. This circuit pack is also used for ISDN-PRI trunk testing (M/T-DIG) and ATMS trunk testing (M/T-ANL).

## Effects of circuit-pack failures on the packet bus

Certain faults of any of the previous circuit packs can disrupt traffic on the packet bus. Some failures cause packet-bus problems with corresponding alarms, while others cause service outages without alarming the packet bus (although the failed circuit pack should be alarmed).

Failures of packet-bus circuit packs affect the bus in the following ways:

- **TN2312AP IP Server Interface (IPSI)** — A failure of an IPSI's Packet Interface circuit typically causes all packet traffic either within its scope or within the PN to fail. As a result:
  - An IPSI-connected PN and its CSS connectivity are disabled.
  - ISDN-BRI sets cannot make or receive calls.
  - Communication with ASAI adjuncts fail.
  - System ports are disabled.
  - ISDN-PRI D-channel signaling is disabled.

  If the Packet Interface circuit's fault is on its packet-bus interface, the packet bus may also alarm.

  In a standard, high-, or critical-reliability system with duplicated IPSIs, one TN2312AP IPSI circuit pack resides in each PN's control carrier. If a fault in the active IPSI's Packet Interface circuit disrupts the packet bus, an IPSI interchange may restore service. In other cases, replacement of the circuit pack may be required before service can be restored.
- **TN570 Expansion Interface (EI)** — A failure of an EI circuit pack typically causes all packet traffic in the connected PN or CSS to fail. If the failure is on its packet-bus interface, the packet bus may be alarmed as well.

  If an active EI failure causes a packet-bus disruption in a critical-reliability system (duplicated PNC), a PNC interchange may restore service. In other cases, replacement of the circuit pack may be required before service is restored.
- **TN556 ISDN-BRI** — A failure of an ISDN-BRI circuit pack typically causes some or all ISDN-BRI sets and data modules and/or an ASAI adjunct connected to the circuit pack to stop functioning. If the failure is on the circuit pack's packet-bus interface, the packet bus may be alarmed.
- **TN464F Universal DS1** — A failure of a Universal DS1 circuit pack disrupts ISDN-PRI signaling traffic carried on the D channel. The loss of that signaling may impact the pack's 23 B channels. If the D channel supports NFAS (non-facility-associated signaling), the B channels of up to 20 other DS1 circuit packs may also be affected. In cases where all 24 channels of the circuit pack are B channels, packet bus-related failures may not affect the B channels, since only D-channel signaling is carried on the packet bus. If the failure is on the circuit pack's packet-bus interface, the packet bus may be alarmed as well.

**TN771D Maintenance/Test** — A Maintenance/Test board's fault may either:

— Falsely indicate a packet-bus fault

— Cause the inability to detect such a fault

If the test board's fault is on its packet-bus interface, the packet bus may also be alarmed.

Failure of any circuit pack's bus interface may alarm the packet bus due to shorting of packet-bus leads. This typically disrupts *all* packet-bus traffic in the affected PN. Some packet-bus faults do not affect every endpoint, so a packet-bus fault cannot be ruled out just because some packet service is still available.

A circuit pack can fail in such a manner that it sends bad data over the packet bus. If this occurs on an:

- IPSI's Packet Interface circuit, all packet traffic either within the IPSI-connected PN or its scope is disrupted.
- EI circuit pack may disrupt all packet traffic in its PN.
- ISDN-BRI circuit pack, every device connected to the circuit pack fails to function.

This failure may also disrupt the entire packet bus whenever the circuit pack tries to transmit data. Such a disruption may be indicated by:

- Intermittent packet-bus alarms
- Intermittent failures of other packet circuit packs
- Interference with other connected endpoints

These failures are difficult to isolate because of their intermittent nature. In most cases, the failed circuit pack is alarmed, and every connected endpoint on the circuit pack is out of service until the circuit pack is replaced. These symptoms help in isolating the fault.

# Packet bus maintenance

The following topics are covered in this section:



## Comparing the packet and TDM buses

The packet and TDM buses have several similarities and differences. There are two physical TDM buses in each PN. One of the buses can fail without affecting the other, but half of the call-carrying capacity is lost. There is *one* packet bus in each PN. A failure of that bus can disrupt all packet traffic in that PN.

In critical-reliability systems, the Maintenance/Test circuit pack provides packet-bus reconfiguration capabilities. This allows the packet bus to remain in service with up to three lead failures. There is no corresponding facility on the TDM bus. Instead, the second physical TDM bus continues to carry traffic until repairs are completed.

System response varies according by type of bus failure and whether or not the failure occurs in a:

- PN controlled by an IPSI-connected PN

  In such a PN, a catastrophic TDM bus failure (one that affects both TDM buses) disables *all* traffic in the PN. A catastrophic packet-bus fault affects only packet traffic, so that TDM traffic is unaffected, while all ISDN-BRI, ASAI, and ISDN-PRI signaling traffic is disrupted.

  The significance of this distinction depends on the customer's applications. A customer whose primary application requires ASAI would consider the switch to be out of service, while a customer with a:

  — Large number of digital/analog/hybrid sets

  — Small number of ISDN-BRI sets

  would probably not consider the packet-bus fault a catastrophic problem. The only way a PN's packet-bus fault can affect TDM traffic is by impacting the system's response time in a large switch while running ISDN-BRI endpoint maintenance. This should rarely happen because the Packet Bus maintenance software can prevent this for most faults (see Packet Bus maintenance software on page 225).

- IPSI-connected PN

  If a packet-bus fault occurs in an IPSI-connected PN, the impact can be more wide-spread. Since an IPSI-connected PN's packet bus can carry the signaling and control links for other PNs, a packet-bus failure in this PN effectively:

  — Disrupts the IPSI-connected PN's packet-bus traffic

  — Removes every subordinate PN within its scope from service, including both TDM and packet buses.

  **CAUTION:**
  Packet-bus fault isolation and correction often involves circuit-pack removal, which is destructive to service. Minimize time devoted to destructive procedures by using non-destructive ones whenever possible.

## Packet Bus maintenance software

PKT-BUS (Packet Bus) contains information about packet bus error conditions, tests, and alarms. Since a PN's packet-bus fault can cause every BRI/ASAI endpoint and its associated port and circuit pack to report faults, be careful to prevent a flood of error messages overloading the system and interfering with traffic on the TDM bus. When such a failure occurs, circuit-pack maintenance is affected in the following manner:

- In-line errors for the following MOs that indicate possible packet-bus faults are logged but *not acted upon:* BRI-BD, PGATE-BD, PDATA-BD, UDS1-BD.
- In-line errors for the following MOs that indicate possible packet-bus faults are *neither logged nor acted upon:* BRI-PORT, ABRI-PORT, PGATE-PT, PDATA-PT, ISDN-LNK.
- All in-line errors for the following MOs are *neither logged nor acted upon:* BRI-SET, BRI-DAT, ASAI-ADJ.
- Circuit pack and port in-line errors that are not related to the packet bus, or that indicate a circuit pack failure, are acted upon in the normal fashion.
- Periodic and scheduled background maintenance is not affected.
- Foreground maintenance (for example, commands executed from the terminal) is not affected.

These interactions allow normal non-packet system traffic to continue unaffected, and they reduce the number of entries into the error/alarm logs. If the packet bus failure is caused by a failed circuit pack, errors against the circuit pack should appear in the error/alarm logs as an aid for fault isolation. The above strategy is implemented when:

- In-line errors indicate a possible packet bus failure reported by two or more packet circuit packs.
- A packet-bus uncorrectable report is sent from the Maintenance/Test packet-bus port (M/T-PKT).

When such a failure occurs, a PKT-BUS error is logged; see PKT-BUS (Packet Bus) for more detailed information.

## General fault correction procedures

This section gives an overview of the procedures used to isolate the cause and to correct packet bus faults. Details are presented in following sections.

1. Procedure 1 attempts to determine whether a circuit pack that interfaces to the packet bus is the cause of the packet bus problem. This involves examination of the error and alarm logs followed by the usual repair actions.
2. If the packet bus problem persists, remove port circuit packs (those in purple slots) to look for circuit packs that have failed and/or damaged the packet bus pins.
3. If the packet bus problem persists, perform the same procedure for control complex circuit packs.
4. If the problem persists, or if the packet-bus faults are known to have open leads, replace bus terminators and cables. If this does not resolve the problem, reconfigure the carrier connectivity of the PN to attempt to isolate a faulty carrier.

## Maintenance/Test circuit pack (TN771D)

The TN771D Maintenance/Test circuit pack provides the following functions:

- Analog Trunk (ATMS) testing
- Digital Port Loopback testing
- ISDN-PRI Trunk testing
- Packet Bus testing
- Packet Bus reconfiguration (critical-reliability systems only)

Critical-reliability systems have a TN771D in each PN. A TN771D is optional in PNs of non-critical-reliability configurations. The ISDN-PRI trunk testing functions are discussed in ISDN-PLK (ISDN-PRI Signaling Link Port).

The digital port testing functions are discussed in:

- DIG-LINE (Digital Line)
- DAT-LINE (Data Line Port)
- PDMODULE (Processor Data Module) TDMODULE (Trunk Data Module)
- TDMODULE (Trunk Data Module)
- MODEM-PT (Modem Pool Port)

The analog trunk testing functions are discussed in the following sections in:

- TIE-TRK (Analog Tie Trunk)
- DID-TRK (Direct Inward Dial Trunk)
- AUX-TRK (Auxiliary Trunk)

**NOTE:**
Every Maintenance/Test circuit pack must be of TN771D vintage or later.

## TN771D packet bus testing functions

The Maintenance/Test packet-bus port (M/T-PKT) provides the packet-bus testing and reconfiguration capabilities. When the port is in service, it continuously monitors the packet bus for faults and fault recoveries, and reports results to PKT-BUS maintenance.

The amber LED on the TN771D Maintenance/Test circuit pack provides a visual indication of the state of the packet bus:

| | |
|---|---|
| **Flashing** | Flashing of the amber LED once per second indicates that there are too many faults for the Maintenance/Test packet-bus port to recover by swapping leads. *The packet bus may be unusable*. If the failures detected are open lead failures, the packet bus may still be operating. |
| **Steady** | The Maintenance/Test packet-bus port has swapped leads on the packet bus to correct a fault. *The packet bus is still operating*. Or, one of the other ports on the Maintenance/Test circuit pack is in use.<br><br>**NOTE:**<br>First busy out the Maintenance/Test circuit pack's ports not used for packet-bus testing before using this circuit pack to help resolve packet-bus faults. This is done by entering **busyout port *UUCSS*01, busyout port *UUCSS*02**, and **busyout port *UUCSS*03**. Be sure to release these ports when the process is completed. |
| **Off** | There is no packet-bus fault present. |

**NOTE:**
It takes 5 to 10 seconds for the LED to respond to a change in the state of the packet bus.

During normal switch operation, the Maintenance/Test circuit pack provides visual feedback of the packet-bus state. When the circuit pack is in stand-alone mode (see TN771D in stand-alone mode on page 228), these visual indications are still present, but the packet bus is never reconfigured. The amber LED either blinks, or is off.

## TN771D in stand-alone mode

In TN771D stand-alone mode, a terminal is connected to the Maintenance/Test circuit pack with an Amphenol connector behind the cabinet. This setup allows direct inspection of the packet bus and identifies shorted or open leads. This mode does not use the usual MT Maintenance User Interface and is therefore available even if switch is not in service. When in stand-alone mode, the TN771D does not reconfigure the packet bus.

## Required hardware

- TN771D: Standard or high-reliability systems may not have a TN771D in each PN. (Use **list configuration** to determine whether this is so.) When this is the case, take one to the site. See the following section, Special precaution concerning the TN771D on page 234.
- Terminal or PC with terminal-emulation software: The EIA-232 (RS-232) port should be configured at 1200 bps with no parity, 8 data bits, and 1 stop bit. This is a ***different*** configuration than the G3-MT. If a terminal configured as a G3-MT is used, change the SPEED field from 9600 bps to 1200 bps on the terminal's options setup menu. (This menu is accessed on most terminals by pressing the CTRL and F1 keys together. On the 513 BCT, press SHIFT/F5 followed by TERMINAL SET UP.) Remember to restore the original settings before returning the G3-MT to service.
- 355A EIA-232 adapter
- 258B 6-port male Amphenol adapter (a 258A adapter and an extension cable can also be used).
- D8W 8-wire modular cable with an appropriate length to connect the 258A behind the cabinet to the 355A adapter. The relevant comcode is determined by the cable's length, as follows:

  7 feet (2.1 m) — 103 786 786

  14 feet (4.3 m) — 103 786 802

  25 feet (7.6 m) — 103 786 828

  50 feet (15.2 m) — 103 866 109

## Selecting a slot for stand-alone mode

When selecting a slot to use for a TN771D in stand-alone mode in a PN that does not already contain one, keep the following points in mind:

- A port circuit slot (indicated by a purple label) should be used. The service slot (slot 0) ***cannot*** be used for stand-alone mode, even though a TN771D might normally be installed there.
- -5 Volt power supply must be available in the carrier. (For a description of carrier's power supply units, refer to CARR-POW (Carrier Power Supply).)
- A slot in a PN's A carrier is preferable if the previous conditions are met.

## Entering and exiting stand-alone mode

While in stand-alone mode, the TN771D's red LED is lit. This is normal and serves as a reminder to remove the TN771D from stand-alone mode.

**CAUTION:**
A TN771D in stand-alone mode must be the only TN771D in the PN. If one is already in the PN, place it in stand-alone mode. Do **not** insert a second TN771D. Otherwise, the system cannot detect the extra circuit pack and will behave unpredictably.

**CAUTION:**
Critical reliability only: if the TN771D packet bus port has reconfigured the packet bus, as indicated by error type 2049 against PKT-BUS, placing the Maintenance/Test in stand-alone mode causes a loss of service to the packet bus. In this case, *this procedure disrupts service*.

For PNs with a TN771D already installed:

1. Ensure that alarm origination is suppressed either at login or by using the command **change system-parameters maintenance**.
2. Attach the 258A 6-port male Amphenol adapter to the Amphenol connector behind the carrier corresponding to the TN771D's slot. Connect one end of a D8W 8-wire modular cable to port 1 of the 258A. Connect the other end of the cable to a 355A EIA-232 adapter. Plug the EIA-232 adapter into the terminal to be used, and turn the terminal on.
3. Reseat the TN771D circuit pack.

**NOTE:**
Critical reliability only: this causes a MINOR OFF-BOARD alarm to be raised against PKT-BUS. This alarm is not resolved until the TN771D's packet bus port (M/T-PKT) is returned to service. To ensure that PKT-BUS alarms have been cleared, it might be necessary to restore the TN771D to normal mode.

For PNs without a TN771D installed:

1. Attach the 258A 6-port male Amphenol adapter to the Amphenol connector behind the carrier corresponding to the slot where the TN771D is to be inserted. Connect one end of a D8W 8-wire modular cable to port 1 of the 258A. Connect the other end of the cable to a 355A EIA-232 adapter. Plug the EIA-232 adapter into the terminal to be used, and turn the terminal on.
2. Insert the TN771D circuit pack into the slot. The system will not recognize the presence of the circuit pack.

If stand-alone mode is entered successfully, the confirmation displays as shown in Figure 66, Stand-alone mode confirmed, on page 230.

**Figure 66: Stand-alone mode confirmed**

```
                    TN771 STAND-ALONE MODE

                (Type "?" at the prompt for help)

Command:
```

**NOTE:**
If the previous display does not appear, check the wiring between the terminal and the TN771D, and the terminal parameters settings. If these are correct, the TN771D may be defective. In such a case, use the following procedures to exit stand-alone mode, and then test the Maintenance/Test circuit pack. Refer to M/T-BD (Maintenance/Test Circuit Pack) and M/T-PKT (Maintenance/Test Packet Bus Port). If the TN771D fails while in stand-alone mode, the message `TN771 circuit pack failed` is displayed, and no further input is accepted on the terminal. The circuit pack must be replaced.

To exit stand-alone mode:

1. Remove the 258A adapter from the Amphenol connector.
2. If the TN771D was installed for this procedure, remove it. Otherwise, reseat the TN771D.
3. If **change system-parameters maintenance** was used to disable alarm origination, re-enable it now.

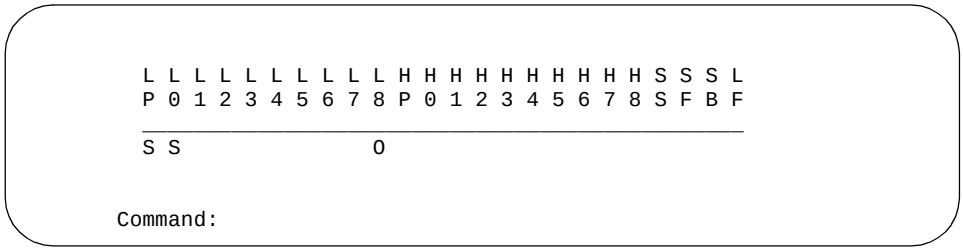
## Packet bus fault isolation and correction in stand-alone mode

When the TN771D is in stand-alone mode, three commands are available:

| | |
|---|---|
| **ds** | Displays the current state of the packet bus leads. |
| **dsa** | Toggles auto-report mode on and off. In auto-report mode, the state of the packet bus leads are displayed and the terminal beeps whenever a change occurs. |
| **?** | Displays the available commands. |

Figure 67, Stand-alone mode display, on page 231 shows the state of the packet bus leads.

**Figure 67: Stand-alone mode display**




- The symbols above the line represent specific leads on the backplane.
- The letters below the line indicate the following:

| | |
|---|---|
| O | Open lead |
| S | Shorted lead. |
| blank | No fault |

**NOTE:**
This information is available only from the stand-alone mode. It is not available from the MT or a remote login.

Figure 68, Packet bus leads on the backplane (front view), on page 232 shows the location of the packet bus leads for a given slot as seen from the front and back of the carrier.

**Figure 68: Packet bus leads on the backplane (front view)**

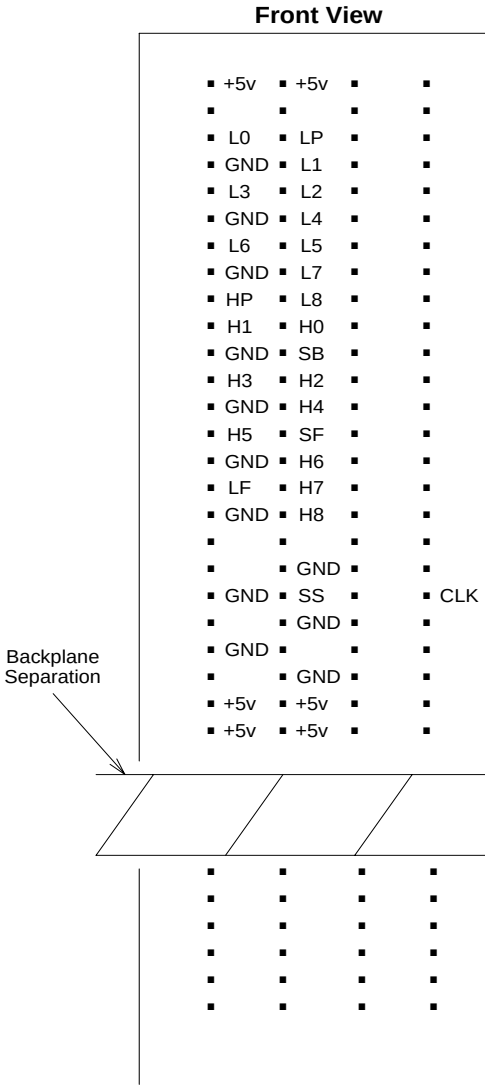
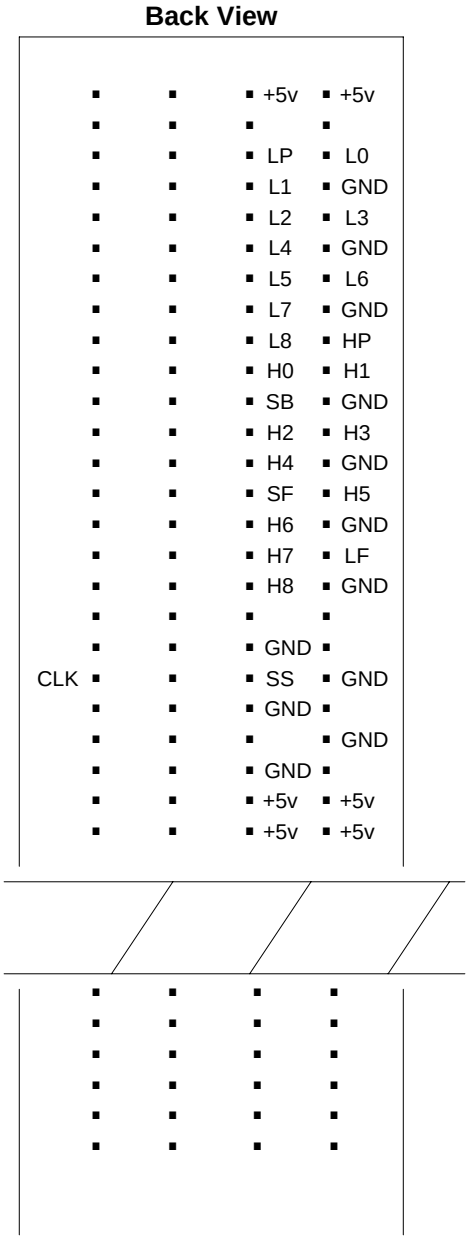


Figure 69, Packet bus leads on the backplane (rear view), on page 233 shows the location of the packet bus leads for a given slot as seen from the front and back of the carrier.

**Figure 69: Packet bus leads on the backplane (rear view)**



### Special precaution concerning the TN771D

A TN771D Maintenance/Test circuit pack must be taken to the customer site if:

- The Maintenance/Test packet-bus port indicates that a packet-bus fault is present by logging a major or minor alarm against PKT-BUS. A major alarm is indicated in the error log by error type 513; a minor alarm is indicated by error type 2049.
- Test #572 of the PKT-BUS test sequence is the only test that fails.

This precaution is taken because certain faults of the Maintenance/Test circuit pack can appear as a packet-bus problem. To ensure that the problem is indeed with the packet bus, proceed through the following steps:

1. If the TN771D Maintenance/Test circuit pack is replaced during this process, enter the **test pkt *P* long** command to determine whether the packet bus faults have been resolved. If not, correct them by using the procedures in the sections that follow.
2. If the Maintenance/Test circuit pack was *not* replaced, enter **test pkt *P***. Record the results (PASS/FAIL/ABORT) and error codes for Test #572.
3. Enter **status port-network *P***. Record the information listed for PKT-BUS.
4. Busyout the Maintenance/Test circuit pack with **busyout board *UUCSS***.
5. Replace the Maintenance/Test circuit pack with the new circuit pack.
6. Release the Maintenance/Test circuit pack with **release board *UUCSS***.
7. Enter the **test pkt *P*** and **status port-network *P*** commands as described in Steps 2 and 3.
8. If the data matches the previously recorded data, a packet bus problem exists, and the original TN771D Maintenance/Test circuit pack is not defective. Reinsert the original TN771D, and correct the packet bus problem by using the procedures in the sections that follow.
9. If the data does *not* match the previously recorded data, the original TN771D circuit pack is defective. If there are still indications of packet bus problems, correct them by using the procedures in the following sections.

## Packet bus fault isolation flowchart

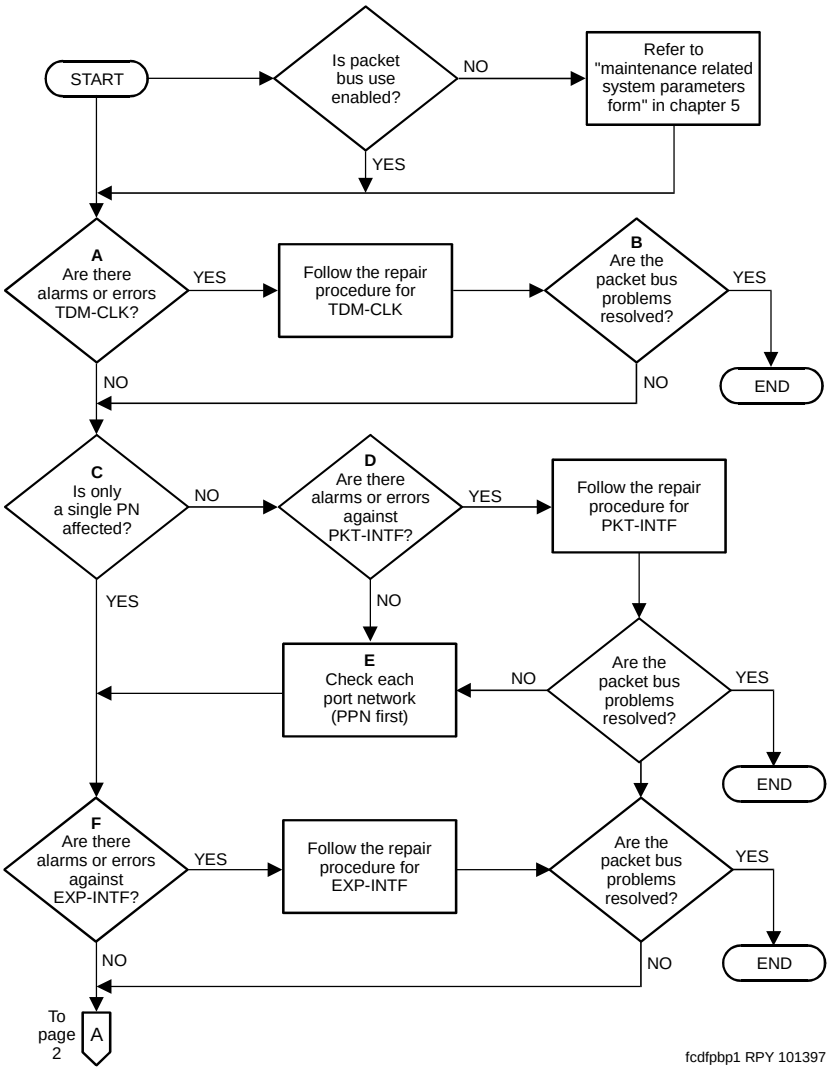
Figure 70, Troubleshooting packet-bus problems (1 of 2), on page 235 and Figure 70, Troubleshooting packet-bus problems (1 of 2), on page 235 show the steps to be taken for isolating and resolving a packet-bus problem. The order of examining maintenance objects (MOs) can be determined by assessing how wide-spread the failure is. For example, since every ISDN-BRI device communicates with the TN2312AP IPSI circuit pack's Packet Interface circuit, its MO should be examined early in the sequence On the other hand, a failure of a PN's TN570 circuit pack may cause an ISDN-BRI failure in one PN, but not in another.

Whenever the flowchart refers to an MO's repair procedure, remember that the repair procedure for that MO may, in turn, refer to another MO's procedure. The flowchart tries to coordinate these procedures so that (if a packet-bus problem is not resolved by the first set of repair procedures) a logical flow is maintained. However, some packet-bus faults can lead to a somewhat haphazard referencing of the various MO procedures — resulting in either repetitive or unnecessary steps. Should this occur, return to

the flowchart at the step that follows the reference to repair procedures and continue from there. The following **status** commands can also help diagnose packet-bus problems, especially when logged in remotely.

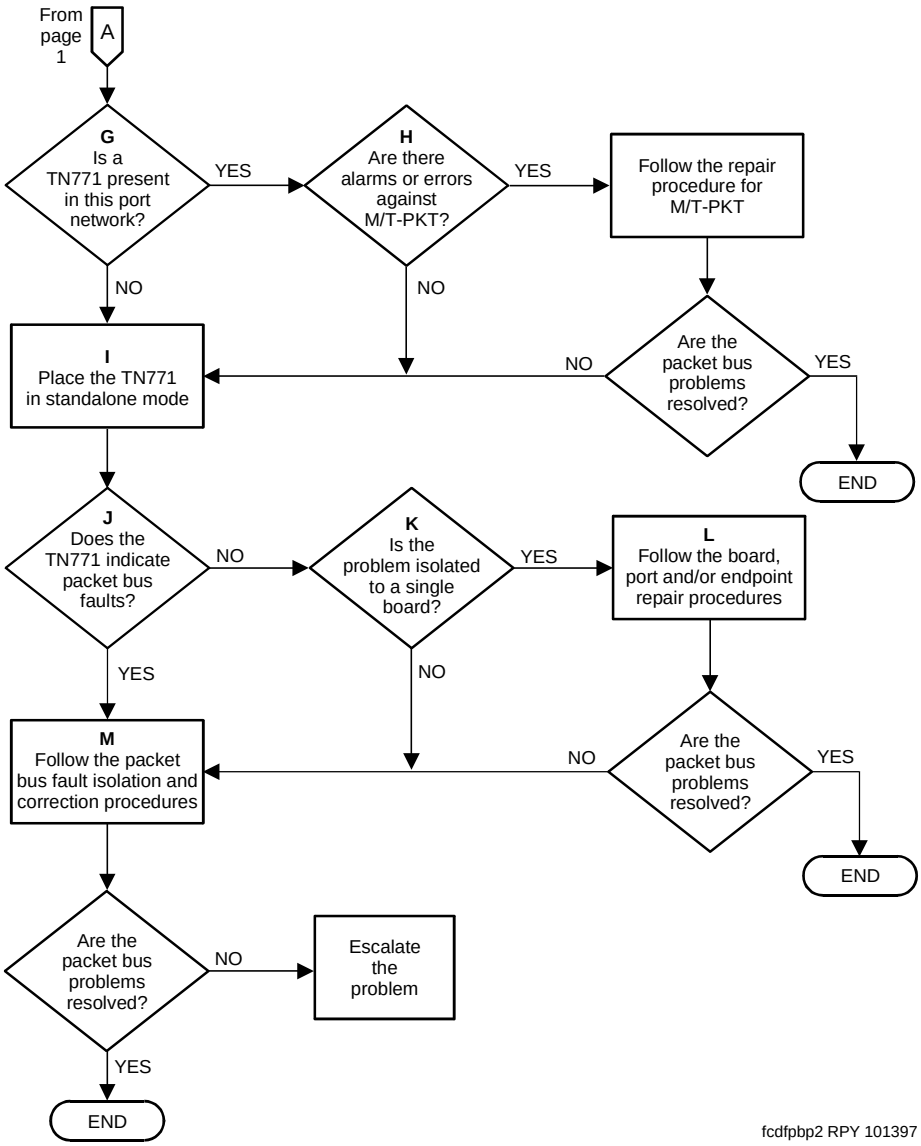
| | |
|---|---|
| status port-network *P* | status ipserver-interface |
| status pnc | status packet-interface |
| status station | status bri-port |
| status link | status data-module |
| status sp-link | status pms-link |
| status journal-link | status cdr-link |

**Figure 70: Troubleshooting packet-bus problems (1 of 2)**



**NOTE:**
Bold-face letters in the flowchart are explained in Flowchart notes on page 236.

**Figure 71: Troubleshooting packet-bus problems (2 of 2)**




**NOTE:**
Bold-face letters in the flowchart are explained in Flowchart notes on page 236.

## Flowchart notes

The following paragraphs refer by letter to corresponding entries in Figure 70, Troubleshooting packet-bus problems (1 of 2), on page 235 and Figure 71, Troubleshooting packet-bus problems (2 of 2), on page 236. Individual errors and alarms are listed in individual maintenance objects. Any that do not refer explicitly to the TDM bus (except TDM-CLK) can be a possible cause of packet-bus problems.

**a** Problems with the system clock (TDM-CLK) can cause service disruptions on the packet bus. Every alarm active against TDM-CLK should be resolved first, even if the explanation refers only to TDM bus. A packet-bus problem cannot cause a TDM-CLK problem, but a TDM-CLK problem can cause a packet-bus problem.

**b** Throughout the flowchart, the question, "Are the packet-bus problems resolved?," refers to the problems that led you to this chart, and can involve several checks, such as:

- Is every packet-bus alarms resolved?
- Is every packet circuit pack's port and endpoint alarm resolved?
- Is every ISDN-BRI station/data module, ASAI adjunct, system port supported adjunct, and ISDN-PRI D-channel link in service?
- Does the Maintenance/Test packet-bus port (in normal or stand-alone mode) still indicate a packet-bus fault?

**c** If only one PN is affected, its Packet Interface circuit is probably not causing the problem. Nonetheless, if every ISDN-BRI and Universal DS1 circuit pack resides in the same PN:

- Assume that the answer to this question is "No."
- Check the IPSI's Packet Interface circuit in this PN.

**d** A packet problem affecting more than one PN is probably caused by either:

- IPSI's Packet Interface circuit fault
- IPSI-connected port network's packet bus fault

If there are IPSI-connected port networks, check the IPSI's Packet Interface circuit before checking the packet bus.

**e** Because each PN's packet bus is physically separate, each affected PN must be checked individually. (However, IPSI-connected PNs should be checked first. Once an IPSI-connected PN's packet problem is resolved, any problems within it's scope are also usually resolved.) After resolving the problem in one PN, verify that problems are also resolved in any other affected PNs.

**f** If a TN771D is absent, one must be installed to accommodate the stand-alone mode. See the previous section on stand-alone mode.

**g** If a TN771D is present, it can fail in such a way that it eventually disrupts the packet bus or misinterprets a packet-bus problem.

**h** If work is being done on-site, follow the procedures described earlier in this discussion on stand-alone mode. If work is not being done on-site, go to the next step.

**i** The answer is "yes" if any of the following apply:

- The TN771D in stand-alone mode indicates any faulty leads.
- Test #572 in the PKT-BUS test sequence fails.
- The **status port-network P** display indicates that faulty leads are present, and the TN771D in the PN is known to be functioning correctly.

**j** If the non-functional endpoints are isolated to a single circuit pack, then that circuit pack is probably the cause of the problem.

**k** Investigate errors and alarms in the following order:

**1** Circuit-pack level

**2** Ports

**3** Endpoints

**l** Follow the Troubleshooting procedures on page 239. If the packet-bus problem cannot be resolved with these procedures, follow normal escalation procedures.

## Correcting packet-bus faults

## Status port-network command

**Status port-network *P*** displays include the service state, alarm status, and (if the Maintenance/Test packet-bus port is present) the number of faulty and open leads for the specified PN's packet bus. This information can be used to determine the urgency of the repair. In general, a service state of "out" indicates extreme urgency, while a service state of "reconfig" indicates moderate urgency.

**NOTE:**
Ultimately, the urgency of a repair is determined by the customer's requirements. A customer who uses ISDN BRI for station sets, or who relies heavily on packet-bus supported system-adjunct features (like DCS, AUDIX, or CDR) probably considers a packet-bus fault critical. On the other hand, a customer with little ISDN-BRI service and no adjunct features may consider even an uncorrectable packet-bus fault less important, and may prefer to delay repairs due to their disruptive nature.

If background maintenance is running on the packet bus when the **status port-network** command is issued, the data reported for the packet bus may be inconsistent due to updating by the tests. If the data seem inconsistent, enter the command again.

If test results or the results of the **status port-network** command indicate that there are 24 faults on the packet bus, the problem is probably caused by faulty cables between carriers, or by defective or missing bus terminators. However, before proceeding, make sure that the Maintenance/Test packet-bus port is not generating a false report by looking for an M/T-PKT error in the error log. Then test the Maintenance/Test packet-bus port with **test port *UUCSSpp***. If any problems are suspected, see Special precaution concerning the TN771D on page 234.

**NOTE:**
If the carrier where a TN771D Maintenance/Test circuit pack is inserted does not have a -5V power supply, the Maintenance/Test packet-bus port reports 24 open leads in response to **status port-network**, or Test #572 of the PKT-BUS test sequence. See CARR-POW (Carrier Power Supply) to ensure that a -5 Volt power supply is available.

**S8700 only**

### Considerations for duplicated systems

Some packet bus-related components are duplicated in systems with one of the duplication options:

- In standard or high-reliability systems (duplicated server, nonduplicated PNC):
  - TN2312AP IPSI circuit packs are nonduplicated in a duplex configuration and duplicated in a high-reliability configuration.
  - A TN771D Maintenance/Test circuit pack is optional in a PN.
  - Maintenance/Test packet-bus reconfiguration is not enabled.
- In critical-reliability systems (duplicated server and PNC):
  - TN2312AP IPSI circuit packs are duplicated.
  - TN771D Maintenance/Test circuit packs are required in every PN.
  - Maintenance/Test packet-bus reconfiguration is enabled.

If a packet-bus problem is caused by a duplicated component, switching to the standby component may alleviate the problem and isolate the faulty circuit pack. Start by executing the commands in the following list when they apply.

- **reset system interchange**: If this command resolves the packet-bus problem, the problem is with the IPSI's Packet Interface circuit that was just switched to standby. Refer to PKT-INT (Packet Interface).
- **reset pnc interchange**: If this command resolves the packet-bus problem, the problem is with the EIs or the link on the PNC (a or b) that just became the standby. Refer to EXP-INTF (Expansion Interface Circuit Pack).
- **set tone-clock**: If this command resolves the packet-bus problem, the problem is with the Tone-Clock that just became the standby. Refer to TDM-CLK (TDM Bus Clock).

Continue with the Troubleshooting procedures on page 239.

## Troubleshooting procedures

Packet-bus faults are usually caused by a defective circuit pack connected to the backplane, by bent pins on the backplane, or by defective cables or terminators that make up the packet bus. The first two faults cause shorts, while the third fault causes either shorts or opens.

There are four procedures for correcting packet-bus faults. The one you use depends on the nature of the fault. For example:

- If the Maintenance/Test packet-bus port is activated, and if there is an indication of open leads on the packet bus from **status port-network** or Test #572, go directly to Procedure 4: isolating failures on page 244. Procedures 1 through 3 try to locate faulty circuit packs or bent pins and these do not cause open faults.
- If there are both shorts and opens, start with Procedure 4: isolating failures on page 244, and return to Procedure 1 if shorts persist after the open leads are fixed.

**CAUTION:**
Packet-bus fault isolation procedures involve removing circuit packs and possibly disconnecting entire carriers. These procedures are destructive. Whenever possible, implement these procedures during hours of minimum system use.

To replace the following circuit packs, follow instructions in the appropriate sections:

- IP-SVR (IP Server Interface)
- EXP-INTF (Expansion Interface Circuit Pack)

When the procedure asks whether the packet-bus problem has been resolved, all of the following conditions should be met:

- Every faulty lead reported by the TN771D's stand-alone mode should no longer be reported.
- Every alarm against the packet bus and the TN2312AP IPSI circuit pack's Packet Interface circuit has been resolved.
- Every ISDN-BRI station and data module **and** every relevant ASAI- and system port-supported adjunct is in service.

## Procedure 1: circuit pack fault detection

Procedure 1 determines whether any circuit packs that use the packet bus have faults. For each circuit pack type in Table 64, Packet circuit packs, on page 240 proceed through the following steps. Check these circuit packs in the order presented by the flowchart shown earlier in this discussion — unless newly inserted circuit packs are involved. Newly added boards are the most likely cause of a problem.

1. **Display errors** and **display alarms** for the circuit pack.
2. For any errors or alarms, follow the repair actions.
3. After following the recommended repair actions, *whether they succeed or fail*, determine whether the packet-bus fault is resolved. If so, you are finished.
4. If the packet-bus fault is still present, apply this procedure to the next circuit pack.
5. If there are no more circuit packs in the list, go to Procedure 2: removing and reinserting port circuit packs.

**Table 64: Packet circuit packs**

| Circuit Pack Name | Code | Associated maintenance objects |
|---|---|---|
| ISDN-BRI | TN556 | BRI-BD<br>BRI-PORT<br>ABRI-PORT<br>BRI-SET<br>BRI-DAT<br>ASAI-ADJ |
| Maintenance/Test | TN771D | M/T-BD, M/T-PKT |

**Table 64: Packet circuit packs**

| Circuit Pack Name | Code | Associated maintenance objects |
|---|---|---|
| Universal DS1 | TN464F | UDS1-BD, ISDN-LNK |
| IP Server Interface (IPSI) | TN2312AP | PKT-INT |
| Expansion Interface | TN570 | EXP-INTF |

## Procedure 2: removing and reinserting port circuit packs

Procedure 2 removes and reinserts port circuit packs (purple slots) and the EI circuit pack one or several at a time. Use Procedure 2 for each port circuit pack in the PN until every port circuit pack has been tried or the problem is resolved.

**NOTE:**
An EI circuit pack should be the last one checked since removing it disconnects the PN. To check an active EI in a critical-reliability system (duplicated PNC), use **reset pnc interchange** to make it the standby. Always check the standby's status before executing an interchange.

**NOTE:**
A Tone-Clock circuit pack should be the next-to-last one checked. (The TN771D must be reseated after the Tone-Clock is reinstalled.) Refer to Procedure 3 on page Procedure 3: removing and reinserting a PN's control circuit packs on page 242 for the TN768, TN780, or TN2182 Tone-Clock circuit pack in a high- or critical-reliability system.

If the packet-bus problem is present when the circuit pack is inserted, but is resolved when the circuit pack is removed, either the circuit pack or the backplane pins in that slot caused the problem. If the backplane pins are intact, replace the circuit pack. Keep in mind that there may be more than one failure cause.

In Procedure 2: removing and reinserting port circuit packs on page 241, you may try one circuit pack at a time, or multiple circuit packs simultaneously. The allowable level of service disruption should guide this choice. If the entire PN can be disrupted, trying large groups of circuit packs will save time. If traffic is heavy, trying one circuit pack at a time is slow but will minimize outages.

If the TN771D's stand-alone mode does *not* indicate packet-bus faults, perform Procedure 2 for *only the port* circuit packs (purple slots) listed in Table 64, Packet circuit packs, on page 240 in Procedure 1. In this case, you need not check for problems with the backplane pins. It is sufficient to determine whether the problem is resolved by removing circuit packs.

If you decide to remove multiple circuit packs, consider working with an entire carrier at a time to more quickly and reliably determine which circuit packs are *not* the source of trouble. Any circuit packs (packet or non-packet) that have been recently inserted should be checked first. Packet circuit packs should be checked before non-packet circuit packs.

1. Remove one or several circuit packs.
2. Determine whether the packet-bus fault is still present. If not, go to Step 4.

3 If the packet-bus fault is still present:

   a Determine whether the backplane pins in the removed circuit pack's slot are bent using the output from the Maintenance/Test circuit pack's stand-alone mode and the backplane illustrations that appear earlier in this discussion.

   b If the backplane pins are bent:

      1 Power down the carrier.

      2 Straighten or replace the pins.

      3 Reinsert the circuit pack.

      4 Restore power.

      5 Repeat Step 2 for the same circuit pack.

   c If the backplane pins are not bent:

      1 Reinsert the circuit pack(s)

      2 Repeat this procedure for the next set of circuit packs.

4 If the packet-bus fault is not present:

   a Reinsert circuit packs one at a time and repeat the following substeps until every circuit pack has been reinserted.

   b Determine whether the packet-bus fault has returned.

   c If the packet-bus fault has returned, the reinserted circuit pack is defective. Replace the circuit pack and then continue.

   d If the packet-bus fault does not return when every circuit pack has been reinserted, you are finished.

Continue with Procedure 3: removing and reinserting a PN's control circuit packs on page 242 if every port circuit pack has been checked, but the packet-bus fault is still not resolved.

**Procedure 3: removing and reinserting a PN's control circuit packs** Procedure 3 removes and reinserts a PN's control circuit packs one at a time. Depending upon the configuration these circuit packs either use the packet bus for communication or are connected to it in the backplane wiring:

- TN2312AP IP Server Interface (IPSI)
- TN768, TN780, or TN2182 Tone-Clock
- PN's TN775 Maintenance

These are the only PN control circuit packs that are likely to cause a packet-bus problem in a stable system. Perform this procedure on only these circuit packs.

If the TN771D stand-alone mode does ***not*** indicate packet-bus faults. Perform Procedure 3 for ***only*** the IPSI or Tone-Clock circuit pack. Do ***not*** check for problems with backplane pins; determining whether the problem is resolved by removing circuit packs is sufficient.

**S8700 only**

## Systems with nonduplicated SPEs

1. Power down the control carrier.
2. Remove the suspected circuit pack.
3. Determine whether the backplane pins in the removed circuit pack's slot are bent.
4. If the backplane pins are bent:
   a. Straighten or replace the pins.
   b. Insert the same circuit pack.

   If not, replace the circuit pack (reinsert the old one if a replacement is not available).
5. Turn the power back and allow the system to reboot. This may take up to 12 minutes. Log in at the terminal.
6. Determine whether the packet-bus fault is still present. If not, you are finished.

If the problem is still present,

a. If the old circuit pack was reinserted in Step 5, replace the circuit pack, and repeat Procedure 3.

b. If the circuit pack was replaced in Step 5, repeat Procedure 3 for the next SPE circuit pack.

If Procedure 3 fails to identify the cause of the problem, go to Procedure 4.

### High- and critical-reliability systems

1. To remove a PN's IPSI circuit pack, use **set ipserver-interface *Uc*** if necessary to make the suspected circuit pack the standby. (Before executing an interchange, always check the status of the standby IPSI's Tone-Clock circuit with **status port-network**.)

   To remove a PN's Tone-Clock circuit pack, use **set tone-clock** if necessary to make the suspected circuit pack the standby. (Before executing an interchange, always check the status of the standby Tone-Clock with **status port-network**.)
2. Determine whether the backplane pins in the removed circuit pack's slot are bent.
3. If the pins are bent:
   a. Power down the carrier if it is not already.
   b. Straighten or replace the pins.
   c. Insert the same circuit pack.
   d. Restore power to the carrier.
4. If the backplane pins are not bent, reinsert or replace the circuit pack.
5. Determine whether the packet-bus fault has been resolved. If so, you are finished.

   If not, do the following:
   a. If the old circuit pack was reinserted in Step 4, replace the circuit pack, and repeat Procedure 3 starting at Step 2.
   b. If the circuit pack was replaced with a new one, proceed with Step 6.

6 Repeat this procedure for the other Tone-Clock. If both have already been checked, continue with Step 7.

7 If every PN control circuit pack has been checked and the problem is still not resolved, continue with Procedure 4: isolating failures on page 244.

## Procedure 4: isolating failures

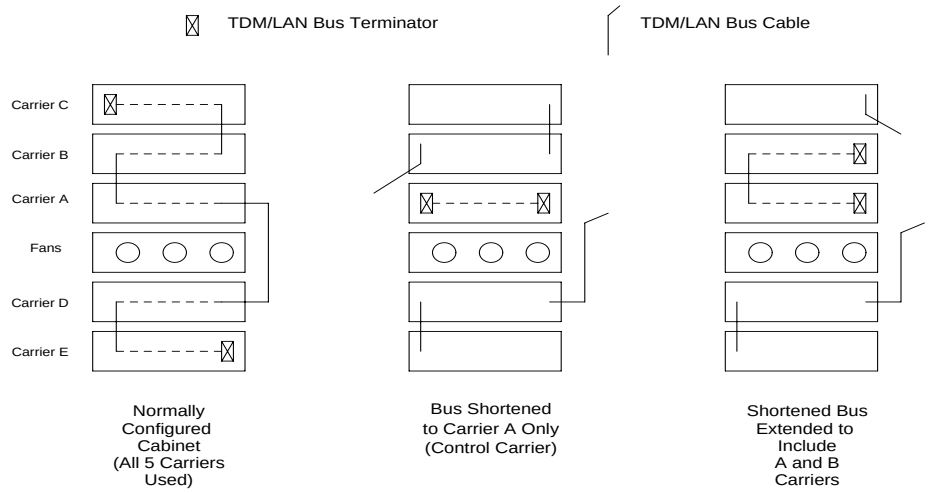
Procedure 4 is used when the preceding procedures fail or when open leads are present. It is helpful in identifying multiple circuit-pack faults and carrier hardware faults. It attempts to isolate the failure to a particular set of carriers and checks only the circuit packs in those carriers.

In Procedure 4, the TDM/LAN cable assemblies and TDM/LAN terminating resistors are replaced. If this action does not resolve the packet-bus fault, the carriers are reconfigured by moving the terminating resistors on the carrier backplanes in such a manner that certain carriers are disconnected from the bus. To terminate the packet bus at the end of a particular carrier, unplug the cable that connects the carrier to the next carrier and replace the cable with a terminating resistor (see Figure 72, Carrier rewiring example—rear view of MCC1, on page 244). When the length of the packet bus is modified with this procedure, circuit packs that are essential to system operation (and the TN771D Maintenance/Test circuit pack in stand-alone mode) must still be connected to the new ‘shortened’ packet and TDM buses.

**DANGER:**
**Power must be removed from the entire port network before any cables or terminators are removed. Failure to do so can cause damage to circuit packs and power supplies, and can be hazardous to the technician.**

**NOTE:**
Circuit packs in carriers that are not part of the shortened bus are not inserted. As a result, these circuit packs are not alarmed. For now, ignore alarm status for these circuit packs. Every alarm should be resolved when the cabinet is restored to its original configuration.

**Figure 72: Carrier rewiring example—rear view of MCC1**



Procedure 4 consists of two parts. Part 1 on page 245 attempts to clear the packet-bus fault by replacing every bus cable and terminator within a PN. Part 2 on page 245 attempts to isolate the fault to a particular carrier by extending the packet bus from the control carrier to additional carriers one at a time.

***Part 1***

1. Power down the PN.
2. Replace every TDM/LAN cable assembly and both of its TDM/LAN terminators.
3. Restore power to the PN.
4. Determine whether the packet-bus fault is still present.
5. If the packet-bus fault is resolved, the procedure is completed. Otherwise, go to Part 2 on page 245.

***Part 2***

1. Place the Maintenance/Test circuit pack into the carrier where the active EI circuit pack resides to isolate the failure to the smallest possible number of carriers.
2. Power down the cabinet and terminate the packet bus on the carrier with the Maintenance/Test (M/T) and active EI.
3. Determine whether the packet-bus fault is still present. If so, and if there are shorts on the packet bus, perform Procedure 2: removing and reinserting port circuit packs and/or Procedure 3: removing and reinserting a PN's control circuit packs for only the circuit packs in carriers connected to the "shortened" packet bus.
4. If the packet-bus fault is not present, extend the packet bus to another carrier, and repeat the procedure in the previous step. When a carrier that causes the fault to recur is added, and if there are shorts, perform Procedure 2: removing and reinserting port circuit packs and/or Procedure 3: removing and reinserting a PN's control circuit packs for only the circuit packs in that carrier.
5. If the packet-bus fault recurs as the packet bus is extended, and if there are no shorts, and Procedures 2 and 3 do not resolve the problem, the added carrier(s) that caused the problem to recur are defective and must be replaced.

---

**8100 only**

# S8100 packet bus fault isolation and repair

**NOTE:**
See // for fault isolation and repair procedures for all other systems.

This chapter describes the fault isolation/correction procedures for the Packet Bus and for the various MOs that use the Packet Bus. Because the Packet Bus is shared by all circuit packs that must communicate on it, a faulty circuit pack can disrupt communication over the Packet Bus. In addition, a circuit pack that does not use the Packet Bus can cause service disruptions if the physical configuration of the switch is being modified (this is discussed in more detail later). For these reasons, isolating the cause of Packet Bus failure can be complicated. In this chapter, a flowchart is provided to aid in this isolation effort, as are detailed discussions of the tools and procedures used in the fault isolation and correction.

This chapter is organized into several sections that provide introductory information, as well as packet bus fault isolation and correction procedures. The sections of the chapter are as follows:

- Remote versus on-site maintenance discusses the strategy and the requirements for performing remote maintenance and on-site maintenance for the Packet Bus.
- Tools for packet bus maintenance discusses the tools that are needed to isolate and correct Packet Bus faults.
- Packet bus describes the Packet Bus, its use, and the types of faults that can occur on the Packet Bus. A diagram that shows the physical and logical connections between circuit packs connected to the Packet Bus is also included.
- Circuit packs that use the packet bus describes the various circuit packs, ports, and endpoints that use the Packet Bus. The section discusses how these maintenance objects interact, how a failure of one maintenance object can affect another, and also the failure symptoms of these maintenance objects.
- Packet bus maintenance describes the Packet Bus maintenance software strategy. Similarities and differences between the Packet Bus and the TDM Bus are discussed. An overview of the Fault Isolation and Correction Procedures is also presented.
- Maintenance/Test circuit pack (TN771D) discusses the use of the Maintenance/Test circuit pack in normal switch maintenance, as well as its role in Packet Bus fault isolation. The standalone mode of the Maintenance/Test (which is used to perform the Packet Bus Fault Isolation and Correction procedures on-site) is discussed in detail.
- Packet bus fault isolation flowchart presents a flowchart that is used to isolate a Packet Bus problem. This flowchart is the starting point for this process, and it is used to determine if a failure of service is caused by the Packet Bus itself or by another maintenance object on the Packet Bus.
- S8100 packet bus fault correction presents the procedures required to correct either a problem with the Packet Bus itself or one that is caused by a circuit pack connected to the Packet Bus.

The Packet Bus Fault Isolation Flowchart is intended to be the normal starting point for isolating and resolving Packet Bus problems. However, anyone who is unfamiliar with Packet Bus maintenance should read the introductory sections to gain a good understanding of the Packet Bus maintenance and the procedures involved.

## Remote versus on-site maintenance

Most packet bus fault isolation and repair procedures require a technician to be on-site. This is true because a packet bus failure is caused by a hardware failure of the packet bus itself or by a circuit pack that is connected to it. However, initial diagnoses can be made via use of the flowchart presented in the Packet bus fault isolation flowchart on page 259 section of this chapter. However, before implementing the Standalone mode on page 253 (described later) and the Packet Bus Fault Correction Procedure, a technician must be on-site.

The flowchart as presented refers to the repair procedures in *Maintenance Alarms Reference (555-245-102)* for various MOs. When one of the decision points is reached, a remote technician can refer to the appropriate section and attempt to resolve any fault conditions. In addition, the remote technician can examine some of the other MOs on the flowchart. Keep in mind that if an MO that appears early on the flowchart fails, this failure can cause alarms with MOs that appear later in the flowchart.

The Maintenance/Test Packet Bus port (described in detail later in this chapter) can give the remote technician information about the state of the packet bus. This information can be obtained with the **status system** command and via the PKT-BUS test sequence. As described later, the Maintenance/Test circuit pack may or may not be present at a customer site, depending on system configuration. If a Maintenance/Test circuit pack is not present, one must be taken to the customer site.

## Tools for packet bus maintenance

The following list discusses several tools that are (or may be) required to perform Packet Bus Fault Isolation and Correction. The technician should be provided with these tools at the customer site:

- TN771 Maintenance/Test circuit pack for use in standalone mode, as well as the required connectors and cables (see the Maintenance/Test circuit pack (TN771D) section).
- Replacement TN771 Maintenance/Test circuit pack may be needed. Conditions for requirement, and the relevant implementation steps are documented in the Special precaution concerning the TN771 section in this chapter.
- Backplane pin-replacement kit may be required in the procedures described in S8100 packet bus fault correction on page 264 of this chapter. If the kit is not available, replacement of a carrier may be required.

## Packet bus

Each port network has its own packet bus, and, accordingly, there is one packet bus MO in each port network. The packet bus is not duplicated, as is the TDM Bus. However, there are several spare leads on the packet bus and, in high and critical reliability systems, these spare leads are used to recover from some failures on the packet bus.

### Packet bus usage

The packet bus carries ISDN-BRI signaling information for ISDN-BRI stations and data modules and for ASAI adjunct connections. The TN556 ISDN-BRI circuit pack is used for these connections. The SPE interface to the packet bus is the TN778 Packet Control (in high and critical reliability systems, there is one TN778 in each SPE). For systems with multiple port networks, the TN570 Expansion Interface is used to pass messages from the packet bus in one port network to the packet bus in its neighbor. The TN771 Maintenance/Test Circuit Pack (discussed in detail later) provides packet bus maintenance testing and reconfiguration capabilities.

### Packet bus faults

Two types of packet bus failures can occur:

- **Shorts**. A short occurs when leads on the packet bus become connected together. Such a connection can occur due to component failures on the packet bus interface of a circuit pack, a failure of the cables between carriers or the TDM/LAN terminators, or by pins being bent together on the backplane. Usually, a failure that occurs during normal operation is caused by a circuit pack failure. However, if the system configuration is being modified (for example, circuit packs are being moved), the cause of a subsequent packet bus failure is probably bent pins.

- **Opens**. An open occurs when there is a break on the packet bus such that the electrical path to the termination resistors is broken. Usually, this break is caused by a failed TDM/LAN cable or by a failed TDM/LAN terminator. The break can also be caused by a failure in the backplane of a carrier, although this is unlikely.

Shorts on the packet bus occur much more often than do opens. This is because the incorrect insertion of a circuit pack can cause leads to be shorted together. It is possible for a circuit pack to be the cause of a packet bus fault but still exhibit trouble-free operation. For example, the insertion of a TDM-only circuit pack (TN754B Digital Line) could bend the packet bus pins on the backplane. However, since the circuit pack does not communicate on the packet bus, the pack is not affected by the problem.

Packet bus faults do not necessarily cause service interruptions. However, most packet bus shorts do cause these interruptions. Depending on what leads are defective, the system may be able to recover and continue to communicate. This can be detrimental because it makes isolating the fault difficult. The Maintenance/Test circuit pack provides the capability to detect, and, in some cases, correct packet bus faults.

### Packet bus connectivity

Various circuit packs communicate on the packet bus. For details on ISDN-BRI and ASAI connectivity, refer to BRI-PORT (ISDN-BRI Port) ABRI-PORT (ASAI ISDN-BRI Port) and BRI-SET, BRI-DAT, Various Adjuncts. For details on Expansion Interface connectivity, refer to EXP-INTF (Expansion Interface Circuit Pack).

## Circuit packs that use the packet bus

Four (4) circuit packs can use the packet bus. The following list identifies and discusses each circuit pack. An explanation of how each circuit pack assists in packet bus maintenance is also included.

> **NOTE:**
> The MOs involved with each circuit pack are listed in brackets. Documentation for each maintenance object is provided in *Maintenance Alarms Reference (555-245-102)*.

- **TN2314 Packet Control** [PKT-INT] provides the SPE interface to the packet bus, just as the TN777 Network Control does to the TDM Bus. All traffic on the packet bus passes through the packet control.

  The packet control can detect failures of certain control leads on the bus. Such failures are indicated by an inability to transmit data. The packet control can also detect data errors on the packet bus.
- **TN556, TN2198 and TN2208 ISDN-BRI circuit packs** [BRI-BD, BRI-PORT, ABRI-PORT, BRI-SET, BRI-DAT, ASAI-ADJ] provides connections for ISDN-BRI station sets and data modules and for ASAI adjuncts. The Packet Bus is used to carry signaling information for sets and data modules. The Packet Bus passes signaling information and ASAI messages between the SPE and the ASAI adjunct. The ISDN-BRI circuit pack has the same fault detection capabilities as the TN570 Expansion Interface.
- **TN771D (or later) Maintenance/Test circuit pack** is the workhorse of packet bus maintenance. This circuit pack can detect all packet bus failures for the PN in which it resides. In High and Critical Reliability systems, the circuit pack enables the reconfiguring of the packet bus

around a small number of failed leads. The TN771D circuit pack provides a standalone mode (that is, one that does not involve communication with the SPE) for inspecting the packet bus for faults. This is a critical tool for the packet bus fault correction procedures, which are described later.

## Effect of circuit pack failures on the packet bus

A failure of any of the circuit packs described in the previous section can disrupt traffic on the Packet Bus. Some failures cause actual Packet Bus failures with corresponding alarms, while others cause service outages without alarming the Packet Bus (although the failed circuit pack(s) should be alarmed).

The following list discusses the effects on the Packet Bus of a failure on each circuit pack that uses the Packet Bus.

- **TN778 Packet Control**. A failure of the Packet Control typically causes all Packet traffic in the system to fail. As a result, ISDN-BRI sets are not able to make or receive calls, and communication with an ASAI adjunct fails. A failure of the Packet Control may also cause a failure of the Packet Bus itself if the failure is on the interface circuitry. Otherwise, only the Packet Control is alarmed.

  In a High or Critical Reliability system, there is one TN778 Packet Control in each SPE. If a Packet Control failure in the active SPE causes a Packet Bus disruption, performing an SPE interchange may restore service. In some cases, circuit pack failures may require that the circuit pack be replaced before service is restored.
- **TN570 Expansion Interface**. A failure of the Expansion Interface typically causes all Packet traffic in the connected EPN to fail. If the failure is on the Packet Bus interface, the Packet Bus may be alarmed as well.

  In a High or Critical Reliability system, there is one EPN link in each control carrier for each EPN. If an active Expansion Interface failure causes a Packet Bus disruption, performing an Expansion Link switch may restore service. In some cases, circuit pack failures may require that the circuit pack be replaced before service is restored.
- **TN556 ISDN-BRI Circuit Pack**. A failure of the ISDN-BRI circuit pack typically causes some or all ISDN-BRI sets and data modules and/or an ASAI adjunct connected to the circuit pack to fail to function. If the failure is on the Packet Bus interface, the Packet Bus may be alarmed as well.
- **TN771 Maintenance/Test**. A failure of the Maintenance/Test may cause an incorrect indication of a packet bus failure or the inability to detect such a failure. A failure of the packet bus interface of the circuit pack may cause the packet bus to be alarmed.

A failure of the packet bus interface on any of the circuit packs discussed can cause the packet bus to be alarmed. This is true because such a failure may result in shorting packet bus leads together. This typically disrupts ALL packet bus traffic in the affected port network. A failure of the packet bus in the PPN affects packet traffic in the EPNs as well. Also, packet bus failures that do not affect all endpoints on that packet bus may occur. Therefore, a packet bus failure should not be ruled out even if some packet service is still present.

A circuit pack can fail in a manner such that it transmits bad data on the Packet Bus. If the Packet Control fails in such a fashion, all Packet traffic is disrupted (because all traffic requires the Packet Control). Likewise, such a failure on the Expansion Interface may disrupt all Packet traffic in that port network.

However, if an ISDN-BRI circuit pack fails such that it transmits bad data, all devices connected to the circuit pack fail to function. This failure may also disrupt the entire Packet Bus whenever the circuit pack tries to transmit data. Such a disruption may be indicated by Packet Bus alarms that occur and go away, intermittent failures of other Packet circuit packs, and/or interference with other connected endpoints. The failures mentioned are difficult to isolate because of their intermittent nature. In most cases, the failed circuit pack is usually alarmed, and all connected endpoints on the circuit pack are out of service until the circuit pack is replaced. These symptoms help in isolating the fault.

# Packet bus maintenance

The following topics are discussed:



## Comparing the packet bus with the TDM bus

Although the Packet Bus is similar to the TDM Bus in many ways, there are some important differences. For example, there are two physical TDM Buses in the switch (refer to the TDM-BUS (TDM Bus) section in *Maintenance Alarms Reference (555-245-102)* for more information), and one of these buses can fail without affecting the other (although half of the call-carrying capacity is lost in this case). On the other hand, there is only a single Packet Bus in the switch, and a failure of that bus can disrupt all traffic on the Packet Bus.

In High or Critical Reliability systems, the Maintenance/Test circuit pack provides Packet Bus reconfiguration capabilities. This allows the Packet Bus to remain in service with up to three lead failures. There is no corresponding facility on the TDM Bus, where the second physical TDM Bus continues to carry traffic until repairs are completed.

In addition, the system response varies according to the type of bus failure. Specifically, a catastrophic TDM Bus failure (one that affects both TDM Buses) disables ALL traffic in the system, while a catastrophic Packet Bus failure affects only Packet traffic. This means that all TDM traffic is unaffected, while all BRI and ASAI traffic does not work. The significance of this distinction depends on the customer's application. (For example, a customer whose primary application requires ASAI would consider the switch to be out of service, while a customer with a large number of Digital/Analog/Hybrid sets and a small number of ISDN-BRI sets would probably not consider the Packet Bus failure a catastrophic problem.) The only way a Packet Bus failure can affect TDM traffic is via possible impact on system response time in a large switch due to ISDN-BRI endpoint maintenance running. This should rarely happen because the Packet Bus maintenance software is able to prevent this impact for most Packet Bus faults (see the next section).

**CAUTION:**
Since the correction procedures and some of the fault isolation procedures for the Packet Bus are highly destructive to service throughout the system (inasmuch as the procedures primarily involve removing circuit packs), particular attention must be paid to nondestructive fault isolation. Also, for the same reason, the time taken with destructive procedures must be minimized. This is the major reason that maintenance of the Packet Bus and of the Packet maintenance objects is described in such detail.

## Packet bus maintenance software

Packet Bus maintenance software involves the traditional set of error conditions, tests, and alarms relevant to Packet Bus faults. These are described in PKT-BUS (Packet Bus - S8100) in *Maintenance Alarms Reference (555-245-102)* and they are similar in design to the maintenance strategy for most maintenance objects.

In addition, because a Packet Bus failure can cause all BRI/ASAI endpoints in the affected Port Network (and their associated ports and circuit packs) to report failures, special care must be taken to ensure that the flood of error messages from the affected maintenance objects does not overload the system and interfere with TDM Bus traffic. When such a failure occurs, maintenance of Packet circuit packs is affected in the following manner:

- ISDN-BRI circuit pack (BRI-BD) in-line errors indicating possible Packet Bus failures are placed into the error log, but are not acted upon.
- ISDN-BRI port (BRI-PORT, ABRI-PORT) in-line errors indicating possible Packet Bus failures **are neither placed into the error log nor acted upon.**
- ISDN-BRI endpoint (BRI-SET, BRI-DAT, ASAI-ADJ) in-line error **are neither placed into the error log nor acted upon.**
- Circuit pack and port in-line errors that are not related to the Packet Bus, or that indicate a circuit pack failure, are acted upon in the normal fashion.
- Normal background maintenance (periodic and scheduled) is not affected.
- Foreground maintenance (for example, commands executed on the Manager I terminal) are not affected.

These interactions allow normal, non-Packet, system traffic to continue unaffected, and they reduce the number of extraneous entries into the Error/Alarm Logs. If the Packet Bus failure is caused by a failed circuit pack, the circuit pack should appear in the Error/Alarm Logs, which aids in fault isolation.

The following events indicate a Packet Bus failure that requires the actions in the previous paragraph to occur:

- In-line errors that indicate a possible Packet Bus failure reported by two or more Packet circuit packs
- Packet Bus Uncorrectable report from the Maintenance/Test Packet Bus port (M/T-PKT)
- Packet Bus Interface Failure from the Packet Control (PKT-INT)

If such a failure occurs, this information is available in the Error Log entry for PKT-BUS. Refer to PKT-BUS (Packet Bus - S8100) section in *Maintenance Alarms Reference (555-245-102)* for more detailed information.

## Fault correction procedure overview

This section gives an overview of the procedures used to (1) isolate the cause of Packet Bus faults and to (2) correct the Packet Bus faults. These procedures are applicable to High and Critical Reliability systems, and they are detailed fully later in this chapter:

1. The first procedure attempts to determine if a circuit pack that interfaces to the Packet Bus is the cause of the Packet Bus problem. The error and alarm logs are examined for entries for these circuit packs, and the normal maintenance procedures for those circuit packs are attempted.

2 If the Packet Bus problem still exists, port circuit packs (those in the purple slots) are removed to look for circuit pack(s) that have failed and/or have damaged the Packet Bus pins (a diagram of the backplane pins is provided later).

3 If the Packet Bus problem is still not resolved, the same procedure is attempted for the control complex circuit packs.

4 If the problem is still not resolved, or if the Packet Bus faults are known to have open leads, a procedure is undertaken in which the bus terminators and cables are replaced. If this does not resolve the problem, the carrier connectivity of the port network is reconfigured to attempt to isolate a faulty carrier.

# Maintenance/Test circuit pack (TN771D)

Packet bus reconfiguration is available only in high and critical reliability systems. In such systems that use the packet bus, a Maintenance/Test is required in each port network. In other configurations (for example, Standard Systems, no packet bus use), the circuit pack is optional.

**CAUTION:**
All TN771 circuit packs must be of TN771D vintage or later.

## Normal packet functionality

The Maintenance/Test Packet Bus Port provides the packet bus testing and reconfiguration capabilities. When the port is in service, the port continuously monitors the packet bus for faults (or recovery from faults), and it reports this information to packet bus maintenance.

The yellow LED on the TN771D Maintenance/Test circuit pack provides a visual indication of the state of the packet bus, as follows:

- **Blinking** at a rate of 1 per sec — the Maintenance/Test Packet Bus port cannot swap leads to correct a Packet Bus fault (that is, there are too many faults). **The Packet Bus may be unusable**. If the failures detected by the Maintenance/Test Packet Bus port are open lead failures, the Packet Bus may still be operating.
- **On steady** — the Maintenance/Test Packet Bus port has swapped leads on the Packet Bus. **The Packet Bus is still operating**.

  **NOTE:**
  Because the yellow LED on the Maintenance/Test circuit pack can also be on steady when the other ports on the circuit pack are in use, the ports on the Maintenance/Test circuit pack used for ISDN-PRI trunk testing must be busied out before the Maintenance/Test circuit pack is used to help resolve Packet Bus faults. This is done via the **busyout port PCSS02** and **busyout port PCSS03** commands. Also, be sure to release these ports when the process is completed.

- **Off** — there is no Packet Bus fault present.

  **NOTE:**
  It takes 5 to 10 seconds for the LED to respond to a change in the state of the Packet Bus.

In normal switch operation, the Maintenance/Test provides the visual feedback of the Packet Bus state. When standalone mode (described in the next section) is in effect, these visual indications are still provided; however, the Packet Bus is never reconfigured, and, as a result, the yellow LED either blinks or is off.

## Standalone mode

The TN771D Maintenance/Test provides a standalone mode for detecting Packet Bus faults. In the standalone mode, a terminal is connected to the Maintenance/Test circuit pack through the Amphenol connector on the back of the cabinet. This setup allows the System Technician to determine the state of the Packet Bus without having to access the Manager I terminal to provide these functions, even if the switch is not in service. Note that the Maintenance/Test does not reconfigure the Packet Bus when it is operating in standalone mode.

Standalone mode is used in the Packet Bus Fault Correction procedures. As a result, **a TN771 and a corresponding terminal must be available to the technician who is to perform such procedures**. A High or Critical Reliability system has a TN771 in each port network. However, the customer of a system that does not have High or Critical Reliability may have purchased a TN771 for ISDN-PRI trunk testing, or to increase the system's ability to detect Packet Bus failures.

The **list configuration** command is used to check for the presence of a circuit pack in the system. If a circuit pack is not present in the system, one must be taken to the customer site. The Special precaution concerning the TN771 section in this chapter discusses the special cases when a spare TN771 must be taken to the customer site.

> **NOTE:**
> When in standalone mode, the yellow LED on the TN771 blinks if there is a Packet Bus fault. If there is no such fault, the yellow LED is off. This is true because Packet Bus reconfiguration cannot occur in standalone mode.

### *Required hardware for standalone mode*

In addition to the TN771, the following equipment is required to use the standalone mode:

- Terminal or PC with terminal-emulation software. The EIA-232 (RS-232) port should be configured at 1200 baud, no parity, 8 data bits, and one stop bit. This is **not** the same configuration as for the Manager I terminal. Therefore, if the Manager I can be used for this operation (and this depends on the switch configuration and on customer requirements), remember to restore the original communication parameters before returning the Manager I to service.
- 355A EIA-232 Adapter
- 258B Six-Port Male Amphenol Adapter
- D8W 8-wire modular cable of an appropriate length to connect the 258A on the back of the cabinet to the 355A adapter.

### *Selecting a carrier slot for standalone mode*

When selecting a carrier slot to use for standalone mode in a port network that does not already contain a TN771, keep the following points in mind:

1. A port circuit slot (indicated by a purple label) should be used.
2. -5 volt power supply must be available in the carrier. This section describes the power supply configurations that provide this power supply.

3 It is preferable that the slot chosen is in the A carrier if a free slot that matches the criteria presented in the first two items of information in this list is available.

### *Entering and exiting standalone mode*

**NOTE:**
When in standalone mode, the red LED on the TN771 is lit. This function is correct, and it serves as a reminder to remove the TN771 from standalone mode.

**CAUTION:**
The TN771 in standalone must be the ONLY TN771 in the port network. If a TN771 is already in the port network, place that TN771 in standalone mode. Do not insert a second TN771 into standalone mode. System behavior is rendered as undefined if this is done. In addition, the system is not able to detect the extra circuit pack in this case because a TN771 in standalone mode is invisible to the SPE.

**CAUTION:**
If the TN771 Packet Bus port has reconfigured the Packet Bus in a switch with a High or Critical Reliability system, (indicated by error type 2049 against PKT-BUS), placing the Maintenance/Test in standalone mode causes a loss of service to the Packet Bus. This is true because reconfiguration is not performed in standalone mode. Therefore, this procedure should be considered a service-disrupting procedure.

If the system has a TN771 installed in the Port Network to be examined, use the following steps to enter the standalone mode:

1 Ensure that Alarm Origination is suppressed either at login time or via the Maintenance-Related System Parameters form.

2 Attach the 258B Six-Port Male Amphenol Adapter to the Amphenol connector for the TN771's slot. Connect one end of a D8W 8-wire modular cable to port 1 of the 258B. Connect the other end of the cable to a 355A EIA-232 Adapter. Plug the EIA-232 Adapter into the terminal to be used, and turn the terminal on.

3 Reseat the TN771 circuit pack.

**NOTE:**
In a High or Critical Reliability system, this causes a Minor, Off-board alarm to be raised against the Packet Bus. This alarm is not resolved until the TN771 (in particular, the Packet Bus port is returned to service. To ensure that Packet Bus alarms have been cleared, it may be necessary to restore the TN771 to normal mode.

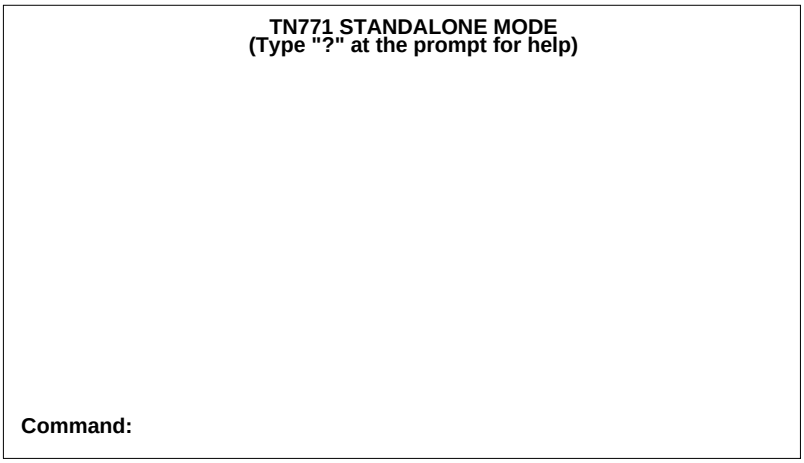
If there is no TN771 in the Port Network, use the following steps to enter the standalone mode:

1 Attach the 258A Six-Port Male Amphenol Adapter to the Amphenol connector for the slot into which the TN771 is to be inserted. Connect one end of a D8W 8-wire modular cable to port 1 of the 258A. Connect the other end of the cable to a 355A EIA-232 Adapter. Plug the EIA-232 Adapter into the terminal to be used, and turn the terminal on.

2 Insert the TN771 circuit pack into the slot. The system does not recognize the presence of the circuit pack.

If the standalone mode is entered successfully, the following is displayed on the connected terminal (Figure 73, Normal standalone mode display, on page 255):

**Figure 73: Normal standalone mode display**




**CAUTION:**
If the display in Figure 73, Normal standalone mode display, on page 255 does not appear, be sure to check the wiring between the terminal and the TN771, and also the terminal parameters. If these are correct, the TN771 may be defective. In such a case, follow the procedures to exit standalone mode (described in the next paragraph). Then test the Maintenance/Test circuit pack.

**NOTE:**
If the TN771 fails while in standalone mode, the message `TN771 circuit pack failed` is displayed, and no further input is accepted on the terminal. The circuit pack must be replaced.

Use the following procedures to exit standalone mode:

1. Remove the 258A Adapter from the Amphenol connector.
2. If the TN771 was installed for this procedure, remove it. Otherwise, reseat the TN771.
3. Be sure that alarm origination is re-enabled on the Maintenance-Related System Parameters form if it was disabled there (if it was disabled at login, it is automatically re-enabled at logoff).

### *Using standalone mode in packet bus maintenance*

When the TN771 is in standalone mode, three commands can be used at the terminal:

- **ds** displays the current state of the Packet Bus leads.
- **dsa** toggles auto-report mode on and off. In auto-report mode, the state of the Packet Bus leads are displayed and the terminal beeps whenever a change occurs.
- **?** displays the available commands.

Figure 74, Example standalone mode display, on page 256 presents an example of a standalone mode display. In the display, an ‘S’ indicates a shorted lead, an ‘O’ indicates an open lead, and a blank indicates no fault.

**Figure 74: Example standalone mode display**

| L | L | L | L | L | L | L | L | L | L | H | H | H | H | H | H | H | H | H | H | S | S | S | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | P | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | S | F | B | F |
| S | S | | | | | | | | | | | | | | | O | | | | | | | |

Command:

The information within a standalone mode display is used in the Packet Bus Fault Correction procedures that follow. The TN771 display indicates the specific leads on the backplane to examine for bent or damaged pins. Figure 75, Packet bus leads on the backplane (front), on page 257 shows the location of the packet bus leads on the backplane as viewed from the front of the carrier, while Figure 76, Packet bus leads on the backplane (back), on page 258 shows the same slot as viewed from the back of the carrier.

**NOTE:**
This information is available only from the standalone mode and with an on-site connected terminal. This information is not available from the Manager I, and, thus, it is not available remotely. This is not a concern, inasmuch as this information cannot be used effectively if testing is not on site.

**Figure 75: Packet bus leads on the backplane (front)**

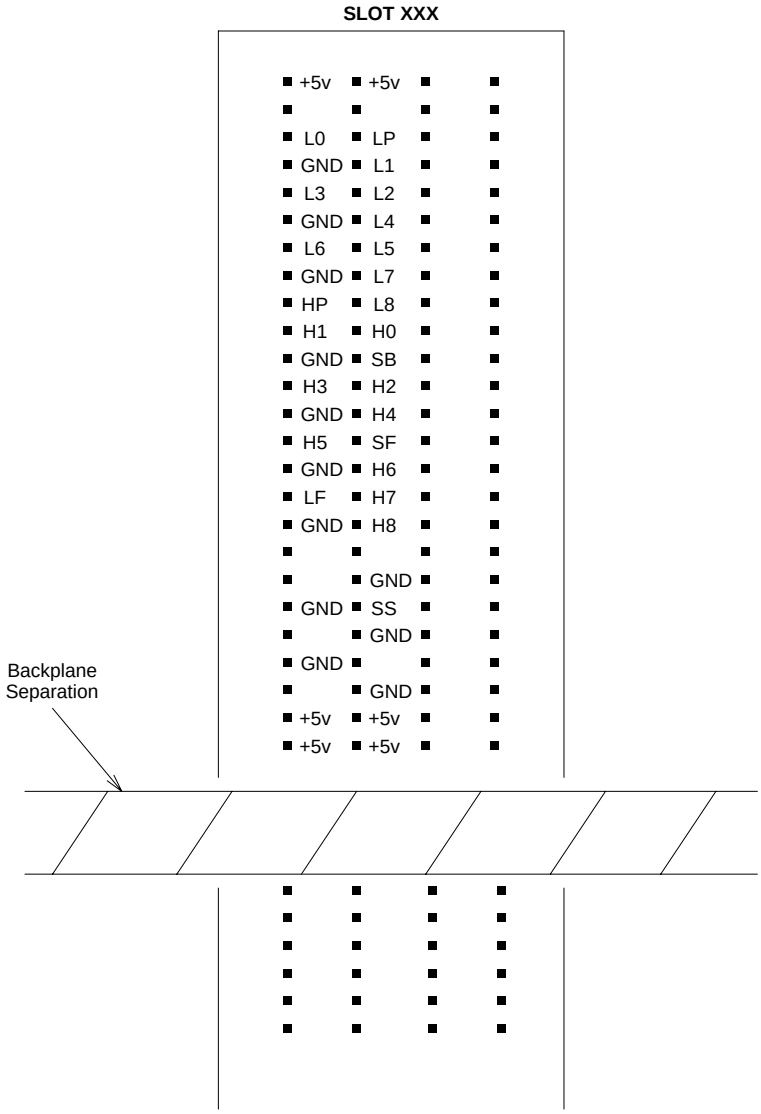
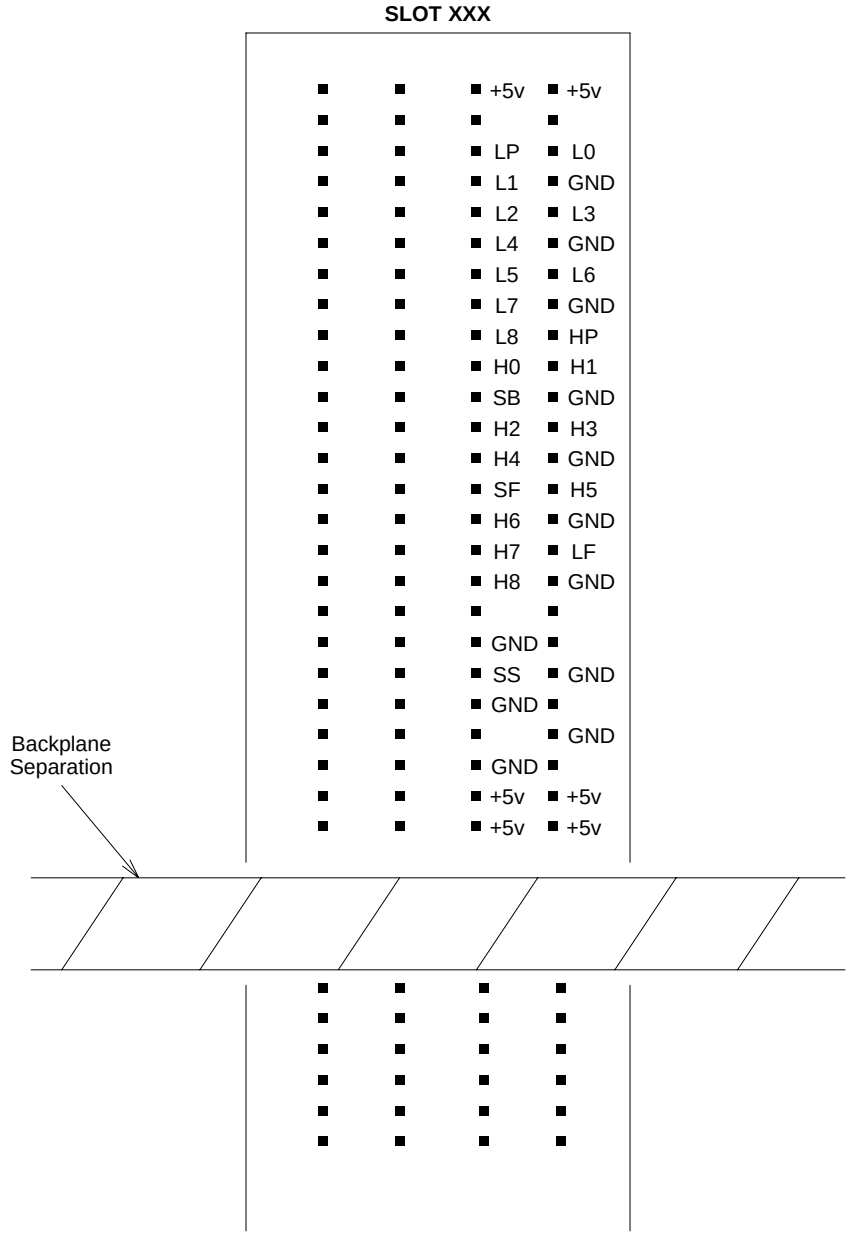


**Figure 76: Packet bus leads on the backplane (back)**




## Special precaution concerning the TN771

**NOTE:**
A new TN771 Maintenance/Test circuit pack must be taken to the customer site whenever the following is true:

- Maintenance/Test Packet Bus port indicates that a Packet Bus fault is present.

  **NOTE:**
  Such a fault is indicated by a Major or Minor alarm against the Packet Bus. A Major alarm is indicated in the error log by Error Type 513, while a Minor alarm is indicated by Error Type 2049.

- Test #572 of the PKT-BUS test sequence is the only test that fails.

This precaution is taken because certain failures of the Maintenance/Test circuit pack can appear as Packet Bus failures. To ensure that the problem is indeed with the Packet Bus, implement the following steps:

1. Refer to M/T-PKT (Maintenance/Test Packet Bus Port) section in *Maintenance Alarms Reference (555-245-102)*. Correct any problems with the TN771 Maintenance/Test Packet Bus port as described in that section. If the TN771 Maintenance/Test circuit pack is replaced during the correction process, enter the **test pkt P long** command to determine if the Packet Bus faults have been resolved. If there are still Packet Bus problems, correct them by using the procedures in the sections that follow.
2. If the Maintenance/Test circuit pack was not replaced, enter the **test pkt P** command. Record the results (PASS/FAIL/ABORT) and error codes for Test #572.
3. Enter the **status system P** command. Record the information listed for the Packet Bus.
4. Busyout the Maintenance/Test circuit pack by entering the **busyout board PCSS** command.
5. Replace the Maintenance/Test circuit pack with the new circuit pack.
6. Release the Maintenance/Test circuit pack by entering the **release board PCSS** command.
7. Enter the **test pkt P** and **status system P** commands as described in Steps 2 and 3.
8. If the data matches the previously recorded data, a Packet Bus problem exists. The original TN771 Maintenance/Test circuit pack is not defective, and it does not need to be returned to the factory. Replace the original TN771, then correct the Packet Bus problem by using the procedures in the sections that follow.
9. If the data does *not* match the previously recorded data, **the original TN771 Maintenance/Test circuit pack is defective**. If there are still indications of Packet Bus problems, correct them by using the procedures in the sections that follow.

## Packet bus fault isolation flowchart

The flowchart in this section presents the steps to be taken for isolating and resolving Packet Bus problems. The order in which the maintenance objects should be examined can be determined by assessing how wide-spread the failure is. For example, since all ISDN-BRI devices communicate with the TN778 Packet Control circuit pack, this MO should be examined early in the sequence. On the other hand, a failure of a TN570 circuit pack in an EPN may cause ISDN-BRI failure in an EPN, but it could not be the cause of a failure in the PPN.

Whenever the flowchart refers to the Maintenance documentation for a specific MO, keep in mind that the repair procedure for that MO may in turn refer to another MO's repair procedure. The flowchart tries to coordinate these procedures so that a logical flow is maintained if the Packet Bus problems are not resolved via the first set of repair procedures. However, a Packet Bus failure can lead to a somewhat haphazard referencing of various MO procedures that may result in your implementing steps that either have already been completed or are not necessary. If this occurs, return to the flowchart at the step that follows the reference to *Maintenance Alarms Reference (555-245-102)*, and then continue.

**NOTE:**
The following **status** commands can also help diagnose Packet Bus problems:

- **status system**
- **status packet-control**
- **status bri-port**
- **status station**
- **status data-module**

For a description of these commands, refer to *Maintenance Commands Reference (555-245-101)*. The commands provide information about the service state of various Packet maintenance objects. This information can be useful for remote maintenance, inasmuch it can explain the impact of the failure(s) on the system.

**NOTE:**
See the Flowchart description and supplement section following the flowchart for a description of the flowchart as well as for supplementary information, the availability of which is indicated by the uppercase letters that appear in the flowchart.

**Figure 77: Packet bus fault isolation flowchart (1 of 2)**

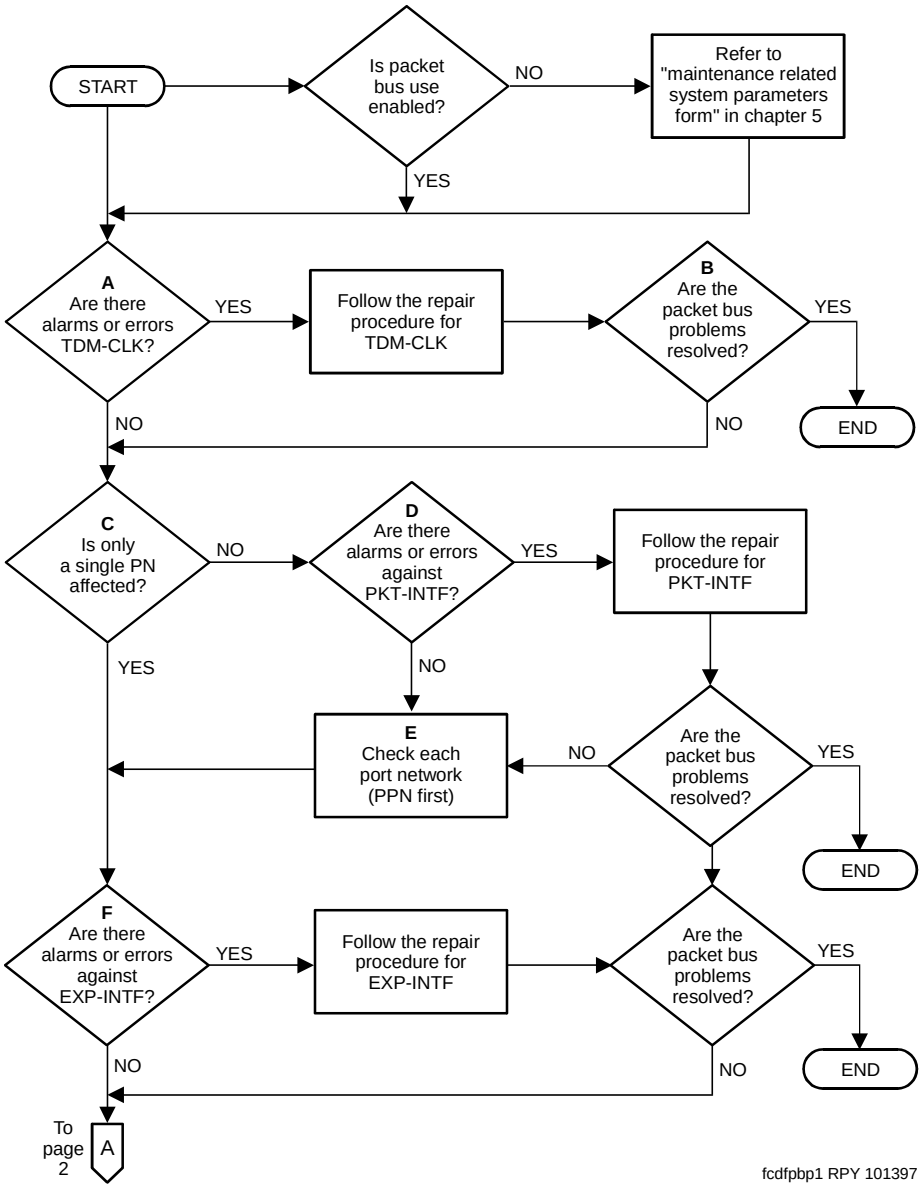
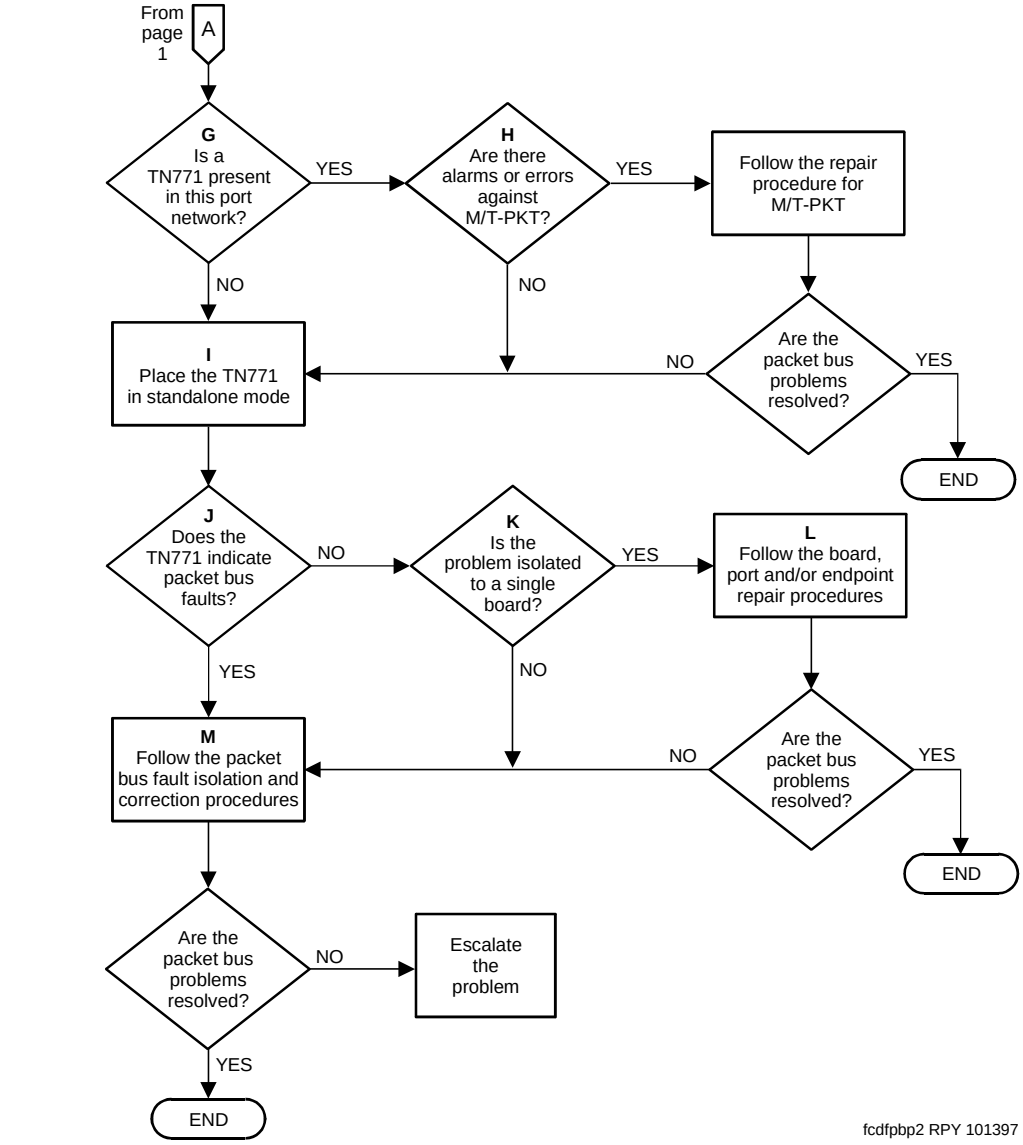


**Figure 78: Packet bus fault isolation flowchart (2 of 2**




## Flowchart description and supplement

An uppercase letter in bold (for example, **A, B, C,** etc.) indicates that there is supplemental information with details about the relevant process that could not fit into the appropriate box or diamond.

**NOTE:**
Due to space restrictions, individual error codes and alarms are not detailed on the flowchart. The maintenance object descriptions in *Maintenance Alarms Reference (555-245-102)*, discuss which errors and alarms could cause or be indicative of Packet Bus problems. In general, unless an error, alarm, or test refers explicitly to the TDM Bus, the error, alarm, or test should be considered a possible cause of Packet Bus problems.

The following paragraphs supplement the corresponding letter in the flowchart.

**a** Problems with the system clock (TDM-CLK) can cause service disruptions on the Packet Bus as well as on the TDM Bus. Therefore, if there are alarms active against TDM-CLK, these alarms should be resolved before any other Packet Bus fault isolation is attempted.

> **NOTE:**
> All TDM-CLK problems should be resolved before the process is continued, even if the problems refer only to the TDM Bus. (This is an exception to the previous note.) This is recommended because a Packet Bus problem cannot cause a TDM-CLK problem, while a TDM-CLK problem can cause a Packet Bus problem.

**b** The question ‘‘Are the Packet Bus problems resolved?’’ appears several times on the flowchart. This is a general question that can involve several checks. The basic question is ‘‘Are the problems that caused you to use this flowchart resolved?’’ Some of the more specific questions might be:

- Are all Packet Bus alarms resolved?
- Are all Packet circuit pack (port, endpoint) alarms resolved?

> **NOTE:**
> If all alarms are resolved, issue the **clear pkt** command. This command attempts to put the switch back into the service state by resolving any BRI problems that exist. Refer to the *Maintenance Commands Reference (555-245-101)* for more information.

- Are all ISDN-BRI stations/data modules and/or ASAI adjuncts in service?
- Does the Maintenance/Test Packet Bus port (in normal or standalone mode) still indicate a Packet Bus fault?

**c** If only a single EPN is affected, the Packet Control is probably not the source of the problem. However, if all of the ISDN-BRI circuit packs are located in a single EPN, assume that the answer to this question is ‘‘No,’’ and check the Packet Control.

**d** A Packet problem that affects more than one port network is probably caused by either a Packet Control failure or a PPN Packet Bus failure. The Packet Control is checked before the Packet Bus Fault Correction procedures are implemented.

**e** Because the Packet Bus in each port network is physically separate, each affected port network must be checked individually. The PPN should be checked first, however, since any EPN Packet problems are usually resolved once the PPN Packet problem is resolved. After resolving the problem in one port network, be sure to check if the problems in other port networks have also been resolved.

**f** This step applies only when an attempt to resolve an EPN Packet Bus problem is made. When checking the Expansion Interfaces in an EPN, be sure to check the corresponding ones in the PPN. Also, recall that all Expansion Interfaces in 286 systems, 386 systems, or later systems that are using the Packet Bus must be TN570s. Using TN776s results in an EPN where TDM traffic works but Packet traffic does not work.

**g** If a TN771 is not present, one must be installed to accommodate the standalone mode, which is discussed earlier in this chapter.

**h** If a TN771 is present, it can fail in such a fashion that it eventually disrupts the Packet Bus or misinterprets a Packet Bus problem.

**i** If work is being done on-site, follow the procedures described Standalone mode on page 253. If work is not being done on-site, go to the next step.

**j** The answer is ‘‘Yes’’ if the TN771 in standalone mode indicates any faulty leads. The answer is also ‘‘Yes’’ if Test #572 in the PKT-BUS test sequence fails, and/or if the **status system** display indicates that faulty leads are present and the TN771 in the port network is known to be functioning correctly.

**k** If the non-functional endpoints are isolated to a single circuit pack, the circuit pack is probably the cause of the problem.

**l** The procedures that must be executed are determined by which maintenance objects on the circuit packs are alarmed. Start with the procedures for the circuit pack errors/alarms, then continue with those for the port. Finally, execute the procedures for the endpoint.

**m** Follow the procedures outlined later in this chapter.

# S8100 packet bus fault correction

## Using and interpreting results from the status system command

The **status system** command can be issued to retrieve information about the Packet Bus. Refer to the *Maintenance Commands Reference (555-245-101)* for more information.

The **status system** command provides the service state, alarm status, and (if the Maintenance/Test Packet Bus port is activated) the number of faulty and open leads. This information can be used to determine the urgency of the repair. In general, a service state of ‘‘out’’ indicates extreme urgency, while a service state of ‘‘reconfig’’ indicates moderate urgency.

**CAUTION:**
Ultimately, the urgency of a repair is determined by the customer’s requirements. A customer who uses ISDN-BRI for station sets probably considers a Packet Bus failure critical. However, a customer with only a small percentage of ISDN-BRI service may consider even an uncorrectable Packet Bus fault to be of minor importance and may prefer to delay performing repairs, due to their destructive nature.

**NOTE:**
If maintenance is actively running on the Packet Bus at the time the **status system** command is issued, the data reported for the Packet Bus may be inconsistent. The reason is that this data is updated by the maintenance tests that are running. If the data seems inconsistent, enter the command again.

If test results or the results of the **status system** command indicate that there are 24 faults on the Packet Bus, the problem is probably caused by faulty cables between carriers, or by defective bus terminators. However, before proceeding, make sure that the report is not being falsely given by the Maintenance/Test Packet Bus port. Accordingly, look for an M/T-PKT error in the error log. Then test the Maintenance/Test Packet Bus port by entering the **test port** command. Refer to the Special precaution concerning the TN771 section earlier in this chapter if any problems are suspected.

If the carrier into which a TN771 Maintenance/Test circuit pack is installed does not have a -5 volt power supply, the Maintenance/Test Packet Bus port reports 24 open leads on the Packet Bus (via the **status system** command and via Test #572 of the PKT-BUS test sequence). No failure of the TN771 is

indicated in this case because the TN771 is not defective. Refer to CARR-POW (Carrier Power Supply) maintenance in *Maintenance Alarms Reference (555-245-102)*, and ensure that a -5 volt power supply is available.

## Troubleshooting procedures

As we discussed earlier in this chapter, Packet Bus faults are usually caused by a defective circuit pack connected to the backplane, by bent pins on the backplane, or by defective cables/terminators that make up the Packet Bus. The first two faults cause shorts, while the third fault causes either shorts or opens.

There are four procedures for correcting Packet Bus faults. The number of procedures that are to be used to correct faults depends upon a number of factors relevant to system performance and to the content of the procedures themselves. For example, if the Maintenance/Test Packet Bus port is activated, and if there is an indication of open leads on the Packet Bus (either via the **status system** command or via Test #572 failure), **go directly to Procedure 4**. The reason for this is that Procedures 1 through 3 try to locate faulty circuit packs or bent pins behind circuit packs. Since these types of failures can never cause open faults, Procedures 1 through 3 need not be implemented in this case. However, if there are both shorts and opens, execute Procedure 4, then return to Procedure 1 if there are still shorts after the open lead problems are resolved.

**CAUTION:**
Since Packet Bus fault isolation procedures involve removing circuit packs and possibly disconnecting entire carriers, these procedure have a profound effect on service. Therefore, if possible, implement these procedures after hours or during hours of minimum system use.

Each of these procedures contains one or more steps that require a determination as to whether the Packet Bus problem has been resolved. Accordingly, several condition checks must be performed. We can present each such check in the form of a question, as follows:

- Did the Maintenance/Test circuit pack standalone mode initially indicate the existence of faulty leads, and are these leads no longer indicated?
- Have all alarms against the Packet Bus and Packet circuit packs been resolved?

  **NOTE:**
  If all alarms are resolved, issue the **clear pkt** command. This command attempts to put the switch back into the service state by resolving any BRI problems that exist.

- Are all ISDN-BRI stations and data modules as well as any relevant ASAI adjuncts in service?

If one of these conditions is not yet met, the others need not be checked. The following sections discuss the four procedures for correcting Packet Bus faults.

### *Procedure 1*

Procedure 1 determines if any circuit packs that use the Packet Bus have faults.

**Table 65: Packet bus circuit packs**

| Circuit Pack Name | Circuit Pack Code | Associated Maintenance Objects |
|---|---|---|
| ISDN-BRI | TN556 | BRI-BD, BRI-PORT, ABRI-PORT, BRI-SET, BRI-DAT, ASAI-ADJ |
| Maintenance/Test | TN771 | M/T-BD, M/T-PKT |

For each circuit pack type (see Table 65, Packet bus circuit packs, on page 266), perform the following steps:

**NOTE:**
The circuit packs need not be checked in the order presented **if the flowchart in this chapter has been followed**. However, if newly added circuit packs are involved, check these packs first, inasmuch as the packs are most likely to have caused a problem.

1. Display the Error and Alarm Logs for the circuit pack via the **display errors** and **display alarms** commands.
2. If there are errors for the circuit pack, refer to the appropriate maintenance documentation in Communication Manager Maintenance-Object Repair Procedures, in *Maintenance Alarms Reference (555-245-102)*, and follow the recommended maintenance procedure to resolve the errors. Note that some of these procedures may refer to PKT-BUS maintenance as the cause of the fault; if so, implement these Packet Bus Fault Correction procedures at that point.
3. After implementing the repair procedure for the circuit pack (and regardless of whether this procedure succeeds or fails), determine if the Packet Bus fault is still present.
4. If the Packet Bus fault is still present, implement Procedure 1 for the next circuit pack.
5. If there are no more circuit packs in the list, go to Procedure 2.
6. If the Packet Bus fault has been resolved, the procedures are completed.

---

### *Procedure 2*

Procedure 2 removes and reinserts port circuit packs (those in the purple slots) one or several at a time. Use Procedure 2 for each port circuit pack in the port network until either (1) the problem is resolved or (2) there are no more circuit packs in the port network.

**NOTE:**
This procedure should also be used for the TN570 Expansion Interface circuit pack in a standard system. For a High or Critical Reliability system, refer to Procedure 3 for the Expansion Interface circuit pack. Also, refer to Procedure 3 for the TN768 or TN780 Tone-Clock circuit pack in a switch with a High or Critical Reliability system.

**CAUTION:**
The Expansion Interface circuit pack should be the last one checked in this procedure, since removing this circuit pack disconnects its EPN. The Tone-Clock circuit pack should be the next-to-last one checked. In addition, the TN771 must be reseated after the Tone-Clock is reinstalled.

If the Packet Bus problem is present when the circuit pack is inserted, but is resolved when the circuit pack is removed, either the circuit pack or the backplane pins in that slot caused the problem. If the backplane pins are intact, replace the circuit pack.

**NOTE:**
In a multiple failure situation, the circuit pack could be one cause of the Packet Bus problem. However, there could also be other failures that are causing Packet Bus faults.

In Procedure 2, an option of working either with one circuit pack at a time or with multiple circuit packs simultaneously is available. In view of this, determine the level of service interruption to be allowed during this procedure. If causing a disruption to all users in the port network is deemed permissible, large groups of circuit packs should be worked with. This option allows faster job completion. **However, if large service disruptions are to be avoided, work with one circuit pack at a time.** This option is slower, but it disrupts only the users of a single circuit pack.

**CAUTION:**
If the TN771 Standalone mode does NOT indicate Packet Bus faults, perform Procedure 2 for ONLY the port (purple) slot Packet circuit packs listed in Table 65, Packet bus circuit packs, on page 266. Also, problems with the backplane pins need not be checked for. Determining if the problem is resolved by removing circuit packs is sufficient.

Steps for Procedure 2

1. Remove one or several circuit packs as appropriate, according to the considerations presented in the previous paragraphs. Any circuit pack(s) (whether Packet or non-Packet) that have been recently inserted should be checked first. It is likely that such a circuit pack caused a new problem. Keep in mind that Packet circuit packs should be checked before non-Packet circuit packs.

   If the decision is made to remove multiple circuit packs, consider working with an entire carrier at a time to ensure a good granularity.

2. Determine if the Packet Bus fault is still present.

3. If the Packet Bus fault is still present:

   a. Determine if the backplane pins in the removed circuit pack's slot are bent. Use the output from the Maintenance/Test standalone mode and Figure 75, Packet bus leads on the backplane (front), on page 257 and Figure 76, Packet bus leads on the backplane (back), on page 258.

   b. If the backplane pins are bent, power down the carrier (see Removing and restoring power on page 391), straighten or replace the pins, reinsert the circuit pack, restore power, and repeat Procedure 2, beginning with Step 2, for the same circuit pack.

**WARNING:**
If this is a High or Critical Reliability system, and if the slot is in the Active control carrier, perform an SPE interchange before changing the circuit pack.

   c. If the backplane pins are not bent, reinsert the circuit pack(s), and perform Procedure 2 for the next set of circuit packs.

4 If the Packet Bus fault is not present, do the following:

   **a** Reinsert a circuit pack. If multiple circuit packs have been removed, reinsert the circuit packs **one at a time**, and repeat the following substeps until all of the circuit packs have been reinserted.

   **b** Determine if the Packet Bus fault has returned.

   **c** If the Packet Bus fault has returned, the reinserted circuit pack is defective. Replace the circuit pack and then continue.

   **d** If the Packet Bus fault does not return when all of the circuit packs have been reinserted, the procedure is completed.

Continue with Procedure 3 if all the port circuit packs have been checked, but the Packet Bus fault is still not resolved.

### *Procedure 3*

Procedure 3 removes and reinserts control carrier circuit packs one at a time. The Packet Control, Tone-Clock, and Expansion Interface circuit packs are the only processor complex circuit packs that communicate on the Packet Bus. In addition, the Memory 1 and EPN Maintenance Board circuit packs are connected to the Packet Bus in the backplane (while the Memory 2 circuit pack is not). Therefore, these are the only processor complex circuit packs that are likely to cause a Packet Bus problem in a stable system. As a result, Procedure 3 should be performed only on the Packet Control, Memory 1, and EPN Maintenance Board circuit packs in all systems, and on the Expansion Interface and Tone-Clock circuit packs in High and Critical Reliability systems.

**CAUTION:**
If the TN771 Standalone mode does NOT indicate Packet Bus faults, perform Procedure 3 for ONLY the Packet Control, Expansion Interface, and Tone-Clock circuit packs. Also, problems with the backplane pins need not be checked for. Determining if the problem is resolved by removing circuit packs is sufficient.

**Standard Reliability only** In a system without High or Critical Reliability, do the following:

1 Power down the control carrier (see. (see Removing and restoring power on page 391).

2 Remove the suspect circuit pack.

3 As in Procedure 2, determine if the backplane pins in the removed circuit pack's slot are bent.

4 If the backplane pins are bent, do the following:

   **a** Straighten or replace the pins

   **b** Insert the same circuit pack

5 If the backplane pins are not bent, replace the circuit pack (reinsert the circuit pack if a replacement is not available).

6 Turn the power back on to reboot the system (see Removing and restoring power on page 391).

7 Determine if the Packet Bus fault is still present.

8 If the Packet Bus fault is still present, do the following:

   **a** If the circuit pack was reinserted in Step 5, replace the circuit pack, and repeat Procedure 3.

   **b** If the circuit pack was replaced in Step 5, repeat Procedure 3 for the next processor complex circuit pack.

9 If the Packet Bus fault does not recur, the procedure is completed.

If Procedure 3 fails to identify the cause of the problem, go to Procedure 4.

**High or Critical Reliability only** In a High or Critical Reliability System, do the following:

1 If the circuit pack to be replaced is in the SPE, perform an SPE interchange by entering the **reset system interchange** command. For an Expansion Interface circuit pack, enter the **set exp-link** command to switch to the standby expansion link. For a Tone-Clock circuit pack, enter the **set tone-clock** command to switch to the standby Tone-Clock circuit pack.

2 Remove the newly-inactive suspect circuit pack. For a circuit pack in the processor complex, use the procedures in the section about Control circuit packs on page 279.

3 As in Procedure 2, determine if the backplane pins in the removed circuit pack's slot are bent.

4 If the pins are bent, do the following:

   **a** Power down the carrier (see Removing and restoring power on page 391).

   **b** Straighten or replace the pins.

   **c** Insert the same circuit pack.

   **d** Restore power to the carrier (see Removing and restoring power on page 391).

5 If the backplane pins are not bent, insert or replace the circuit pack.

6 Determine if the Packet Bus fault is still present.

7 If the Packet Bus fault is still present, do the following:

   **a** If the circuit pack was reinserted in Step 5, replace the circuit pack. Then repeat Procedure 3, starting at Step 2.

   **b** If the circuit pack was replaced in Step 5, continue with Step 9.

8 If the Packet Bus fault does not recur, then the procedure is completed.

9 If the suspect circuit pack has been tested in the other control carrier, go to Step 10. Otherwise, implement Step 1, then Steps 2 through 8.

10 Repeat the procedure in the previous step for the next suspect circuit pack.

If all processor complex circuit packs have been checked and the problem is not resolved, continue with Procedure 4.

### *Procedure 4*

Procedure 4 tries to isolate the failure to a particular set of carriers. Only the circuit packs in those carriers are checked. Procedure 4 is used if the preceding procedures fail, because it can help locate multiple circuit pack failures as well as failures of the carrier hardware. The procedure is also used if there are open leads on the Packet Bus. (The faults detected by Procedures 1 through 3 cannot cause open leads.)

In Procedure 4, the TDM/LAN Cable Assemblies and TDM/LAN termination resistor packs are replaced. If this action does not resolve the Packet Bus fault, the carriers are reconfigured by moving the termination resistor packs in such a manner that certain carriers are disconnected from the bus. This is done by moving the termination resistors on the carrier backplanes. To terminate the Packet Bus at the end of a particular carrier, first unplug the cable that connects the carrier to the next carrier and then replace the cable with a termination resistor (see Figure 79, Carrier rewiring example, on page 270). When the length of the Packet Bus is modified via this procedure, circuit packs that are essential to system operation (for example, Processor Complex, Tone-Clock) must still be connected to the new "shortened" Packet (and TDM) Bus. In addition, the Maintenance/Test circuit pack (in standalone mode) must be connected to the "shortened" bus.

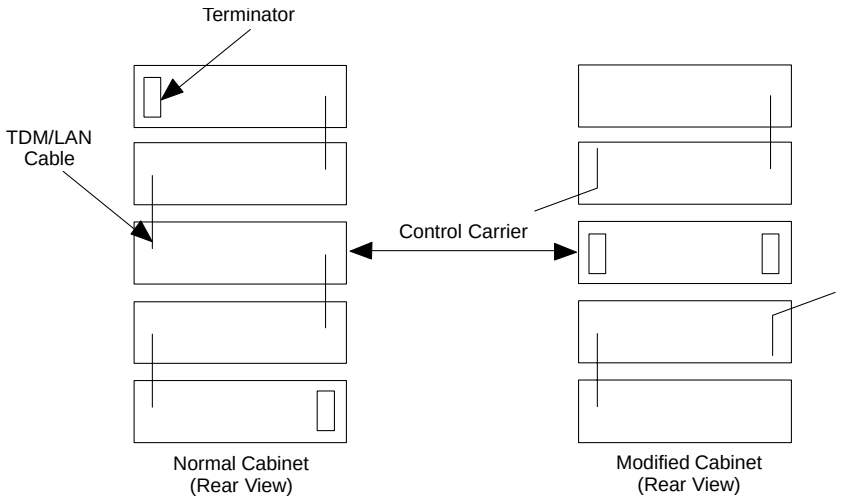
**WARNING:**

Power must be removed from the entire port network before any cables or terminators are removed. Failure to do so can cause damage to circuit packs and power supplies and can be hazardous to the technician. After cabling changes are made and verified, power must be restored to the port network. Use the TN771 Standalone mode to determine if the Packet Bus fault is resolved.

**CAUTION:**

Circuit packs in carriers that are not part of the shortened bus are not inserted. As a result, these circuit packs are not alarmed. Ignore these alarms for now. All alarms should be resolved when the cabinet is restored to its original configuration.

**Figure 79: Carrier rewiring example**




Procedure 4 is organized into two parts, as follows:

***Part 1***

1. Power down the PN (see Removing and restoring power on page 391).
2. Replace all of the TDM/LAN cables and both TDM/LAN terminators.
3. Restore power to the PN (see Removing and restoring power on page 391).
4. Determine if the packet bus fault is still present.
5. If the fault is present, go to Part 2.

***Part 2***

**Processor Port Network**

1. Terminate the Packet Bus so that it extends only from the Active control carrier (that is, the carrier that contains the Active SPE) to the carrier that contains the Maintenance/Test circuit pack. To allow this procedure to isolate the failure to the smallest possible number of carriers, place the Maintenance/Test circuit pack into a carrier that contains a processor complex, if possible.

2 Determine if the Packet Bus fault is still present. If so, and if there are shorts on the Packet Bus, perform Procedure 2 and/or Procedure 3 for only the circuit packs in those carriers that are connected to the ‘‘shortened’’ Packet Bus. (Procedure 2 is performed for port circuit packs, and Procedure 3 is performed for processor complex circuit packs.)

3 If the Packet Bus fault is not present, extend the Packet Bus to another carrier, and repeat the procedure in the previous step. When a carrier that causes the fault to recur is added, and if there are shorts, perform Procedure 2 and/or Procedure 3 for only the circuit packs in that carrier.

4 If the Packet Bus fault recurs as the Packet Bus is extended, and if Procedures 2 and 3 (if performed) do not resolve the problem, the added carrier(s) that caused the problem to recur are defective and must be replaced.

**Other Port Networks**

1 Terminate the Packet Bus so that it extends only from the carrier that contains the Active Expansion Interface to the nearest carrier that contains the Maintenance/Test circuit pack. Place the Maintenance/Test circuit pack into a carrier that contains an Expansion Interface circuit pack in order to allow the procedure to isolate the failure to the smallest possible number of carriers.

2 Determine if the Packet Bus fault is still present. If so, and if there are shorts on the Packet Bus, perform Procedure 2 and/or Procedure 3 for only the circuit packs in those carriers that are connected to the ‘‘shortened’’ Packet Bus.

3 If the Packet Bus fault is not present, extend the Packet Bus to another carrier, and repeat the procedure in the previous step. When a carrier that causes the fault to recur is added, and if there are shorts, perform Procedure 2 and/or Procedure 3 for only the circuit packs in that carrier.

4 If the packet bus fault recurs as the packet bus is extended, and if Procedures 2 and 3 (if performed) do not resolve the problem, the added carrier(s) that caused the problem to recur are defective and must be replaced.

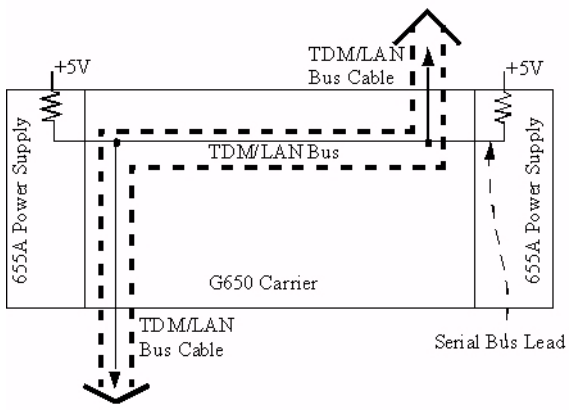
# G650 Serial Bus fault detection and isolation

Each port network of G650s has a Serial Bus that allows the IPSI-2 (TN2312BP) to talk to the 655A power supplies. This Serial Bus uses 2 previously-unused leads in the Universal Port Slot:

- SPARE3 (pin 055) is I2C_SDA (Serial Data).
- SPARE4 (pin 155) is I2C_SCL (Serial Clock).

Older TDM/LAN cables did not have these 2 leads, so the G650 required a new TDM/LAN cable. These 2 leads are not terminated on the TDM/LAN terminators (AHF110). This is an open-collector bus where each power supply and each IPSI-2 provide a pull-up resistor to +5VDC for each of the 2 Serial Bus leads. The bus has logic pulses extending between 0V and 5V. One of the IPSI-2s acts as master of the Serial Bus and polls each of the power supplies based on their board address, which is derived from 4 board address leads in the power slot of the backplane. The G650 carrier addressing paddle card sets 3 of these 4 address leads for the power slot.

**Figure 80: TDM/LAN bus connection to the Serial Bus**




Serial Bus faults can be caused by

- A defective circuit pack connected to the inserted into one of the G650 slots.
- Bent pins on the G650 backplane.
- Defective TDM/LAN bus cables.

It is possible that a circuit pack can cause a Serial Bus fault and still exhibit trouble-free operation. For example, insertions of any circuit pack into a G650 slot might bend the backplane pins and short two leads together. Or a circuit pack that doesn't use the Serial Bus could still have an on-board short of one of the Serial Bus leads. Since the Serial Bus is a shared resource that each circuit pack and power supply has access to, identification of the cause of a Serial Bus fault can be difficult.

**WARNING:**
Since the Serial Bus fault isolation procedure involves removing circuit packs and possibly disconnecting entire carriers, the procedure is extremely destructive to the port network that is being tested. If possible, arrange to perform this procedure at a time when traffic is minimal.

As circuit packs are removed or entire carriers are disconnected, any active calls terminating on those circuit packs or carriers are dropped. If you have any hints about a particular circuit pack that might be causing the Serial Bus problem

- Investigate those suspect circuit packs before performing either procedure. For example, look at any circuit packs that were inserted into the PN just before the Serial bus problem appeared.
- Examine which power supplies that the system is unable to show with the **list configuration power-supply *cabinet*** and concentrate on those carriers and their cabling.

**WARNING:**
When straightening or replacing backplane pins in a carrier, power to that carrier must be shut off. Failure to follow this procedure may result in damage to circuit packs and power supplies and can be hazardous to the technician.

## Procedure 1

This procedure removes and reinserts port circuit packs (those in the purple slots) one or more at a time. Use this procedure for each port circuit pack in the port network until the problem is resolved or until all circuit packs in the port network have been tried.

If the Serial Bus problem is present when the circuit pack is inserted, but is resolved when the circuit pack is removed, either the circuit pack or the backplane pins in that slot are causing the problem. If the backplane pins are intact, replace the circuit pack. If some of the tests fail, regardless of whether the circuit pack is inserted or removed, and the backplane pins are intact, the circuit pack is not the cause of the problem. In a multiple failure situation, the circuit pack could be one cause of the Serial Bus problem. However, other simultaneous failures might also be responsible for Serial Bus faults. In Procedure 2 an option of working either with one circuit pack at a time or with multiple circuit packs simultaneously is available. In view of this capability, determine the level of service interruption that will be acceptable during the procedure. If causing a disruption to all users in the port network is deemed permissible, large groups of circuit packs should be worked with in order to get the job done quickly. However, if large service disruptions are to be avoided, work with one circuit pack at a time. This option is slower, but it disrupts only the users of a single circuit pack.

1. Remove one or several circuit packs as appropriate. Any circuit packs that have been recently inserted should be checked first. If you decide to remove multiple circuit packs, consider working with an entire carrier at a time to more quickly and reliably determine which circuit packs are not the source of trouble. Do not remove the A carrier IPSI-2, as it is the link back to the server.
2. Run **list configuration power-supply *cabinet*** to determine if some power supplies are still not showing and the Serial Bus fault is still present.
3. If the fault is still present:
   a. Check if the backplane pins in the removed circuit pack's slot appear to be bent.
   b. If the backplane pins are not bent, reinsert the circuit pack(s), and perform Procedure 1 for the next set of circuit packs.
   c. If the backplane pins are bent, remove power to this carrier in the manner described previously.
   d. Straighten or replace the pins and reinsert the circuit pack.
   e. Restore power and repeat Step 2, for the same circuit pack(s).
4. If the fault is not present:
   a. Reinsert the circuit pack(s) one at a time, and repeat the following substeps until all of the circuit packs have been reinserted.
   b. Run **list configuration power-supply *cabinet*** to determine if the Serial Bus fault has returned.
   c. If any of the power supplies don't show, the reinserted circuit pack is defective. Replace this circuit pack and repeat this procedure for the next circuit pack.
   d. If none of the power supplies fail to show when all of the circuit packs have been reinserted, the problem has been fixed and the procedure is completed.

## Procedure 2

Procedure 2 attempts to isolate the Serial Bus failure to a particular set of carriers. Only the circuit packs in selected carriers are checked. Procedure 2 is used if Procedure 1 fails, because it can help locate multiple circuit pack failures and failures of the carrier hardware itself. In this procedure, the TDM/LAN

cable assemblies and TDM/LAN bus terminators are replaced. If this action does not resolve the Serial Bus fault, the carriers are reconfigured so that certain carriers are disconnected from the Serial Bus. This is done by moving the TDM/LAN bus terminators (AHF110) on the carrier backplane. To terminate a Serial Bus at the end of a particular carrier, the Serial Bus cable that connects the carrier to the next carrier should be unplugged and replaced with the TDM/LAN Bus terminator. When the length of the Serial Bus is modified, the A carrier IPSI-2 circuit pack that is essential to the Serial Bus operation and Serial Bus maintenance must still be connected to the new, shortened Serial Bus.

After making and verifying the cabling changes, restore power to the port network. Circuit packs in carriers that are not part of the shortened bus are not inserted, and as a result these circuit packs are alarmed. Ignore these alarms for now. All alarms should be resolved when the cabinet is restored to its original configuration.

Procedure 2 is organized into two parts:

- Part 1 attempts to clear the Serial Bus fault by replacing all the bus cabling and terminators within a port-network.
- Part 2 attempts to isolate the fault to a particular carrier by extending the Serial Bus from the A carrier to additional carriers one at a time.

**WARNING:**
Remove power from the entire port network before removing any cables or terminators. Failure to follow this procedure can cause damage to circuit packs and power supplies and can be hazardous to the technician.

## Part 1

1. If spare TDM/LAN cable assemblies and TDM/LAN Bus Terminators are not available, go to Part 2 of this procedure.
2. Power down the port network.
3. Replace all of the TDM/LAN cable assemblies and both TDM/LAN bus terminators.
4. Restore power to the port network.
5. Run the **list configuration power-supply *cabinet*** command to determine if the Serial Bus fault is still present.
6. If the Serial Bus fault is resolved, the procedure is completed. Otherwise, go to Part 2.

## Part 2

1. Terminate the TDM/LAN Bus so that it extends only across the carrier that contains the A carrier IPSI-2.
2. Determine if the Serial Bus fault is still present by running the **list configuration power-supply *cabinet*** command.
3. If **list configuration power-supply *cabinet*** doesn't fail to show any power supplies, extend the TDM/LAN/Serial Bus to another carrier, and repeat the procedure in the previous step. When a carrier that causes the fault to recur is added, perform Procedure 2 for only the circuit packs in that carrier.
4. If **list configuration power-supply *cabinet*** fails to show any power supplies, and neither procedure has resolved the problem, the added carrier(s) are defective and must be replaced.

# 8 Component replacement

This chapter describes how to replace components in the system. It includes the following topics:



## Variable-speed fans

A variable-speed fan is identified by the following features:

- A fan and air filter assembly with product code ED-67077-30, Group 4 or greater, labeled on the front of the carrier
- A 5-pin white connector mounted next to each fan on the fan assembly cover plate for speed control and alarm circuitry
- A 2-pin black -48 V power connector to each fan
- A power filter (ED-1E554-30, G1 or G2) located in a metal box mounted behind the fans on the right-hand cable trough as you face the rear of the cabinet
- The AHD1 circuit pack and the two S4 sensors used with older fan assemblies are *absent*.

Alarm leads from each fan are tied together into a single lead that registers a minor alarm against CABINET whenever a fan's speed drops below a preset limit or fails altogether.

**NOTE:**
The front fans may run at a different speed than the rear fans since they are controlled by different sensors.

## Replacing variable-speed fans

This procedure applies to replacement of a variable-speed fan (KS-23912, L3) in a new type fan assembly (ED-67707-30, G4 or greater). Do *not* use a constant-speed fan in this assembly.

1. If replacing a fan in the front of the cabinet, remove the white plastic fan assembly cover by pulling it outward. There is no cover on the rear fans; they are accessible simply by opening the rear cabinet doors.
2. *Connect the grounding wrist strap to yourself and the cabinet.* The fan alarm circuit can be damaged by ESD.
3. Disconnect the white 5-pin connector on the fan assembly.
4. Loosen and remove the retaining screw nearest the power connector on the defective fan.
5. Disconnect the 2-pin black power plug on the fan.
6. Loosen and remove the other retaining screw on the fan.
7. Remove the fan from the fan assembly.
8. Position the new fan and insert the screw that is opposite the power connector.
9. Connect the 2-pin black power plug on the fan.
10. Connect the white 5-pin connector on the fan assembly. Insert and tighten the retaining screws.
11. Replace the front fan cover, if removed.

## Replacing the fan power filter

The fan power filter (ED-1E554-30) is a metal box located behind the fans on the right-hand cable trough as you face the rear of the cabinet. It is absent with constant-speed fan assemblies.

**CAUTION:**
The fan power filter can be replaced without powering down the cabinet. To avoid damage, you must use the following steps in the order shown. Note that the J2F/P2F connectors on the power filter must not be connected whenever connecting or disconnecting the J2/P2 connectors on the fan assembly.

1. Access the power filter through the rear cabinet doors.
2. *Connect the grounding wrist strap to yourself and the cabinet.* The fan alarm circuit can be damaged by ESD.

**CAUTION:**
Failure to disconnect the J2F connector on the filter before the J2 connector on the fan assembly can damage the fan alarm circuits.

3 Disconnect cabinet local cable connector J2F from the P2F connector on top of the power filter.

4 Disconnect cable connector J2 from the P2 connector on the fan assembly.

5 Loosen the power filter mounting screws using a 5/16” nut driver and remove the filter.

**CAUTION:**
Failure to connect the J2 connector on the fan assembly can damage the fan alarm circuits.

6 Connect the J2 cable connector of the replacement power filter to the P2 connector on the fan assembly.

7 Mount the new power filter on the screws and tighten.

8 Connect cabinet local cable connector J2F to the P2F connector on the top of the power filter.

9 The fans should start rotating after a 4 second delay.

## Replacing the temperature sensor

The top temperature sensors are located at the top rear of the cabinet in some cabinets. On these cabinets, the removable media shelf is located on the rear door, at the bottom.

1 From the rear of the cabinet, remove the screws holding the top temperature sensor.

2 Replace the sensor with a new one using the screws removed above.

3 Route the cable along the path of the existing sensor cable.

4 Unplug the cable on the defective sensor and replace with the plug on the new sensor.

5 Remove the old sensor from the cabinet.

# Reseating and replacing circuit packs

Most repair procedures involve replacing faulted circuit packs. In some cases, problems are resolved by reseating the existing circuit pack. Reseat a circuit pack ***only*** when explicitly instructed to do so by the documented procedures. Reseating is discouraged since it can put a faulty component back into service without addressing the cause, resulting in additional and unnecessary dispatches. After reseating a circuit pack, make sure the problem is really fixed by thoroughly testing and observing the component in operation.

When a port board is removed from the backplane, no alarm is logged for about 11 minutes to allow for maintenance activity to proceed. After that, a minor on-board alarm is logged. If the port board is not administered, no alarm is logged.

**WARNING:**
This procedure can be destructive, resulting in a total or partial service outage.

**WARNING:**
Proceed only after consulting and understanding the applicable service documentation for the component.

**WARNING:**
If the amber LED on the circuit pack to be removed is lit, the circuit pack is active, and services using it will be interrupted.

## Special procedures

**CAUTION:**
Table 66, Circuit packs requiring special reseating or replacing procedures, on page 278 lists the circuit packs that require special procedures for reseating and replacing and a link to the specific reseating/replacing information:

**Table 66: Circuit packs requiring special reseating or replacing procedures**

| Circuit pack | Description | Link to information |
|---|---|---|
| TN2312AP | IP Server Interface (IPSI) | IP-SVR (IP Server Interface)<br>If the IPSI has a static IP address, refer to the "Reusing a TN2312AP circuit pack" section in *Installing the Avaya S8700 Media Server with an Avaya G650 Media Gateway, 555-245-109* for reseating and replacement procedures. |
| TN768<br>TN780<br>TN2182B | Tone-Clock<br>Tone-Clock<br>Tone-Clock for a PN without an IPSI | TONE-BD (Tone-Clock Circuit) (all) |
| TN570 | Expansion Interface | EXP-INTF (Expansion Interface Circuit Pack) |
| TN573 | Switch Node Interface | SNI-BD (SNI Circuit Pack) |
| TN572 | Switch Node Clock | SNC-BD (Switch Node Clock Circuit Pack) |
| DS1 CONV | DS1 Converter | DS1C-BD |

**S8100**

# S8100 component maintenance

## Reseating/replacing S8100 circuit packs

**WARNING:**
It is NOT recommended that you reseat circuit packs unless the documentation specifically instructs you to do so. If it is required to reseat a circuit pack, follow the instructions below which explain how to unseat, reseat, and replace circuit packs.

The procedures for unseating, reseating, and replacing control circuit packs vary depending on the system configuration. Therefore, before performing these maintenance activities, refer to the appropriate procedure below.

## Control circuit packs

### *To unseat a control circuit pack*

1. Remove power from the PPN using the procedure provided in Hardware shutdown on page 394.
2. Slide the latch pin upward to unlock the locking lever.
3. Pull down on the locking lever until the circuit pack disconnects from its socket.
4. Pull the circuit pack just enough to break contact with the backplane connector, but do not remove it from the cabinet.

### *To reseat a circuit pack*

1. Push the unseated circuit pack back into the backplane connector.
2. Lift the locking lever until the pin engages.
3. Restore power to the PPN using the procedure provided in Restoring power on page 394.

### *To replace control circuit packs*

1. Remove power from the PPN using the procedure in Hardware shutdown on page 394.
2. Unseat the circuit pack.
3. Slide the circuit pack out of the slot.
4. Replace the circuit pack as per the following procedure:

**NOTE:**
If a new circuit pack does not correct the problem, install the original circuit pack.

### *To install a new circuit pack or return the original one to service*

1. Carefully insert the circuit pack and push it all the way into its mounting slot.
2. Lift the locking lever until the latch pin engages.
3. Restore power to the cabinet using the procedure in Restoring power on page 286.
4. Verify that the circuit pack LED indications are correct.
5. Test the replaced control circuit pack by issuing the system technician commands after power has been restored.

## Replacing the TN2314 circuit pack

**WARNING:**
When the TN2314 circuit pack is replaced, the system enters License-Error mode. A new license file and password file must be downloaded and installed on the system within six days in order to restore the system to License-Normal mode. Otherwise, the system enters No-License mode, and normal call processing is blocked. Refer to Installing License and Authentication files on page 91 for more information.

### *Save translations*

1. Connect the laptop to the S8100.
2. Click Start > Run.
3. Type **telnet** *name* in the dialog box, where ***name*** is the local name of your TN2314 system processor.
4. In the **Enter your login name** dialog box, type **lucent1**, **lucent2**, or **lucent3**, and click OK.
5. In the **Enter password** dialog box, type the appropriate password for the login used, and click OK.

   A LAC prompt displays (LAC>).
6. Type **definity**

   You automatically login to *name* **Definity**.
7. Select terminal type NTT (for Windows 2000, select terminal type W2KTT).
8. From the command line, type **save translations**
9. After saving translations successfully, type **logoff** to log off the Definity.
10. Close the telnet window.

### *System shutdown*

1. Click Start > Run.
2. Type **bash** in the dialog box.

   A prompt such as *name*-**lucent1**> displays.
3. Type **shutdown system**
4. Type **d1stat** to check the status of the shutdown.

   DEFINITY, INTUITY AUDIX, and Audixnet should show DOWN; CORNERSTONE should show partially UP.
5. When the shutdown is complete, type **exit** to close the bash window.
6. Remove the TN2314 circuit pack.
7. Remove the hard disk from the failed TN2314 circuit pack.
8. Insert the hard disk onto the new TN2314 circuit pack.

   **NOTE:**
   Do not use the hard disk from the TN795 circuit pack.

9. Plug in the new TN2314 board.

   The system boots automatically.

   **NOTE:**
   The system enters License-Error mode, because the serial number on the new processor no longer matches the serial number stored with RFA. Refer to License-Error on page 94 for more information.

10. Use the web-based RFA to download new License and Authentication files (see Downloading the License and Authentication files on page 91).
11. After the license and password files have been installed and the system has been rebooted, login to the system and run a demand test on the new board.

12 Check for proper operation
   - Alarms
   - Trunk status
   - INTUITY functionality

## Replacing fans and air filters (CMC1)

Air filters on the CMC1 should be inspected annually. (See Table 67, Inspecting air filters, on page 281.)

**Table 67: Inspecting air filters**

| If | Then |
|---|---|
| Filter is dirty or clogged | Tap filter on the ground. |
| Tapping does not dislodge dirt or clog | Wash with warm water and mild detergent, or clean with a vacuum cleaner (if one is available). |
| No facility exists for washing or vacuuming | Replace air filter. Refer to Figure 81, Fan/filter removal, on page 282 for more information on air filters and fans. |

### Fan filter removal/replacement

1 Remove the left door.

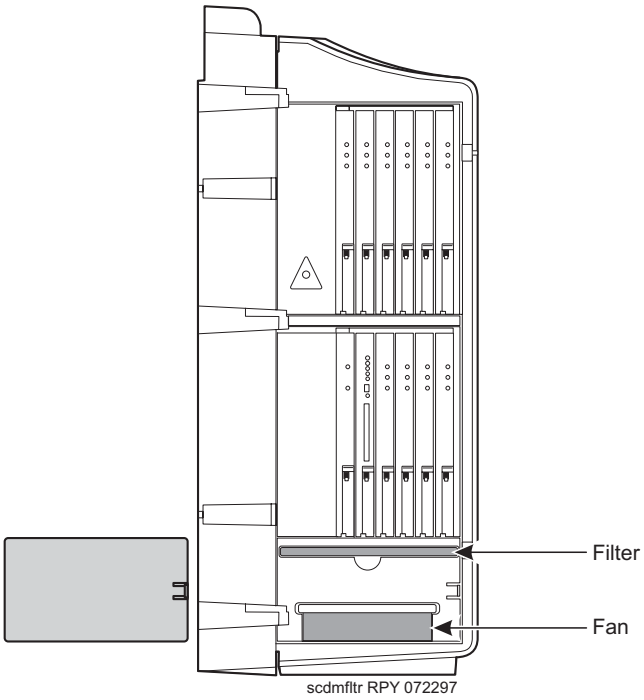
2 Remove the fan access panel from the left side of the cabinet.

3 Pull the fan filter from the chassis (Figure 81, Fan/filter removal, on page 282).

4 Clean (vacuum or wash with water) or replace the filter as needed and slide the filter back into the chassis.

5 Replace the fan access panel.

**Figure 81: Fan/filter removal**




## Fan assembly removal/replacement

1. Pull (unplug) the fan assembly from the chassis. The power for the fan automatically disconnects when the assembly is unplugged.
2. Plug in the new fan assembly. The power for the fan automatically connects when the fan assembly is plugged in.
3. Replace the fan/filter access panel and the left door.

## Replacing the S8100 hard disk

**NOTE:**
When the TN2314 hard disk is replaced, the system remains in License-Normal mode, because the serial number of the processor remains the same. However, a copy of the License and Authentication files must be obtained from RFA. Refer to Downloading the License and Authentication files on page 91 for more information.

Sections in this procedure include:

## Shutdown AUDIX

1. Connect the laptop to the S8100.
2. Click Start > Run.
3. Type **telnet** *name* in the dialog box.
4. In the **Enter you login name** dialog box, type **lucent1**, **lucent2**, or **lucent3**, and click OK.
5. In the **Enter password** dialog box, type the appropriate password for the login used, and click OK.

   A LAC prompt displays (LAC>).
6. Type **bash**

   The bash window displays a prompt such as *name*-**lucent1**>.
7. From the bash window, type **shutdown audix**

   **NOTE:**
   You might see an error message stating that a “clean shutdown not possible. Forced termination of process” This means that there was probably someone retrieving INTUITY messages when you shutdown AUDIX. the shutdown will proceed normally, anyway.
8. Wait for the bash prompt.
9. Type **d1stat** to make sure INTUITY AUDIX is DOWN.

   Audix and Audixnet should show DOWN.
10. Type **exit** to leave the bash window.

    A LAC prompt displays (LAC>).

## Save translations

1. Type **definity**

   You automatically login to *name* **Definity**.
2. Select terminal type NTT.
3. From the command line, type **save translations**
4. After saving translations successfully, type **logoff** to log off the server.
5. Close the telnet window.

## Backup the S8100

For information about how to start a web browser, see the procedure, “Via a Web Browser Session” in Chapter 2, “Connectivity and Access” in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

1. Login to S8100 using Internet Explorer browser.

   The URL is: http://*hostname*

   Note: hostname is the name of the S8100 switch.
2. Click on the **Administer System** link.
3. Login, using **lucent1**, **lucent2**, or **lucent3**, with your current password assignment.

4 Click OK.

5 Click the **Continue** button.

6 click on the **Backup & Restore** link (under System Maintenance).

7 Click on the **Immediate Backup** link.

8 Select the desired items for immediate backup (i.e., Communication Manager translation files; INTUITY translations, names, and messages).

9 Verify that the backup destination shows **pcmcia**.

10 Click on the **Backup** button.

11 Click on the **View Backup Progress** icon at the bottom of the page to view backup progress.

> **NOTE:**
> If INTUITY translations, names, and messages have been selected, the INTUITY networking stops during the backup procedure.

12 After the backup completes successfully, close **Internet Explorer**.

## System shutdown

1 Click Start > Run.

2 Type **bash** in the dialog box.

A prompt such as *name*-**lucent1**> displays.

3 Type **shutdown system**

4 Type **d1stat** to check the status of the shutdown.

DEFINITY, Audix, and Audixnet should show DOWN; CORNERSTONE should show partially UP.

5 When the shutdown is complete, type **exit** to close the bash window.

6 Remove the TN2314 circuit pack.

7 Remove the failed hard disk from the TN2314 circuit pack.

8 Insert the new hard disk onto the new TN2314 circuit pack.

> **NOTE:**
> You cannot use the hard disk from the TN795 circuit pack.

9 Insert the TN2314 board.

The system boots automatically.

> **NOTE:**
> The disk comes pre-loaded with all the necessary S8100 software; however, the S8100 applications won't run until you install copies of the license and password files. Since the TN2314 processor serial number remains the same, it is not necessary to obtain new license and password files. However, these files are not on the new hard disk; therefore, you must contact RFA for copies of the original files to be downloaded and installed.

10 Once the system has rebooted, connect the services laptop computer to S8100.

11 Connect the laptop to the S8100.

12 Click Start > Run.

13 Type **telnet** *name* in the dialog box.

14 In the **Enter you login name** dialog box, type **lucent1**, **lucent2**, or **lucent3**, and click OK.

15 In the **Enter password** dialog box, type the appropriate password for the login used, and click OK.

A LAC prompt displays (LAC>).

16 Type **bash**

The bash window displays a prompt such as *name*-**lucent1**>.

17 Type **swversion**

Verify that the load of software on the hard drive matches that on the customer's CD. If it does not match, follow the Update Software procedure in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways, 555-233-146*.

18 Bring up **Internet Explorer** on the laptop and load the S8100 Home Page. Navigate the browser to the backup and restore screens.

The browser prompts for a login and password, because the new hard disk does not have a password file. The system reverts back to the factory default login of **lucent3**, with **lucent3** as the password.

19 Follow the steps for restoring the customer's data.

> **NOTE:**
> The customer may have backed up to their local network or the PCMCIA flash disk.

20 After restoring, follow the procedures to install License and Authentication files, including running the **loadlicense** command. For more details, Installing License and Authentication Files on page 92.

After installing the License and Authentication files, the system restarts and all applications load.

21 Note that the Windows 2000 logins of **vm**, **sa**, **browse**, and **Ntadmin** will be reset to their factory defaults. Tell the customer to reset these passwords and re-install any other Windows 2000 accounts they may have created.

> **NOTE:**
> The Communication Manager-specific customer logins should still work as they were restored with the restore done earlier.

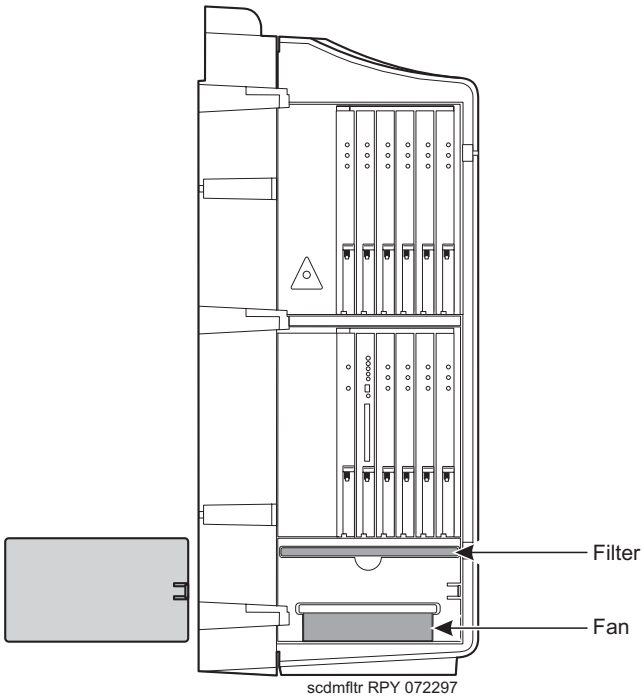
22 If it is necessary, upgrade the software on the disk. If you are upgrading to a new release, the upgrade requires installing new License and Authentication files.

## S8100 fan/filter removal/replacement

1 Remove the left door.

2 Remove the fan/filter access panel as shown in Figure 82, S8100 fan/filter removal, on page 286.

**Figure 82: S8100 fan/filter removal**




## Removing or replacing the S8100 fan assembly

1. Pull (unplug) the fan assembly from the chassis using the thumb/finger notch provided. The power for the fan automatically disconnects when the assembly is unplugged.
2. Plug in the new fan assembly. The power for the fan automatically connects when the fan assembly is plugged in.
3. Replace the fan/filter access panel and the left door.

## Removing or replacing the S8100 fan filter

1. Remove the fan access panel from the left side of the cabinet.
2. Pull the fan filter from the chassis.
3. Clean (vacuum or wash with water) or replace the filter as needed and slide the filter back into the chassis.
4. Replace the fan access panel.

# S8300 and G700 component maintenance

Maintenance of the G700 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.

Replacement procedures in this section include:

- Replacing the G700 Media Gateway on page 290
- Replacing the S8300 Media Server or hard drive on page 290
- Replacing Media Modules on page 299
- Replacing Avaya Expansion Modules on page 301
- Replacing an Avaya Octaplane Stacking Module on page 302

## Field-replaceable components

In addition to Media Modules, the following components on the G700 are field-replaceable. Failure of other components (such as the power supply, fans, or motherboard) requires replacing the entire box. Table 68, Equipment List: G700, on page 287 and Table 69, Equipment list: G700 power cords, on page 288 show the G700 field-replaceable components.

**NOTE:**
In the tables to follow, comcodes containing the letter “R” at the end refer to “refurbished” components. If refurbished components are not in stock, the order automatically switches to new equipment.

**Table 68: Equipment List: G700**

| **G700** | | |
|---|---|---|
| | Apparatus Code: MGW1 | Not Optional |
| **G700 ComCode (for Maintenance Ordering Only)** | | |
| **ComCode** | **Number of Items** | **Description** |
| 700259898R | 1 | G700 |
| The following field replaceable components are contained in 700259898R | | |
| 108934316R | 1 | LED Module |
| 700181831R | 1 | Mounting Kit |
| 700216864R | 1 | CLI Cable |
| 700216856R | 1 | CLI Adapter |
| 700057060R | 3 | Media Module Blank |
| 700179195R | 1 | Avaya Expansion Blank |
| 700170203R | 1 | Avaya Octaplane Blank |

**Table 68: Equipment List: G700 — *Continued***

| G700 | | |
|---|---|---|
| 700169998R | 1 | LAN Cable |
| 700228273R | 1 | Ground Cable |
| 700236680R | 1 | Grounding Kit |

**Table 69: Equipment list: G700 power cords**

| G700 Power Cords | | |
|---|---|---|
| Material Code: 170904 | Apparatus Code: none | Not Optional |
| When you order this material code, a descriptive attribute will be required; the attributes are: | | |
| **Attribute** | **Option** | **Comcode: Description** |
| CRD | 30 | 405362641: PWR CORD 9X10 IN USA 17505 |
| CRD | 31 | 407786623: PWR CORD 98IN EUROPE 12013S |
| CRD | 32 | 407786599: PWR CORD 98IN UNITED KINGDOM 14012 |
| CRD | 33 | 407786631: PWR CORD 98IN AUSTRALIA 15012 |
| CRD | 34 | 407790591: PWR CORD INDIA P250CIM |
| CRD | 42 | 408161453: PWR CORD 96IN ARGENTINA |

# Processors

If it necessary to replace the Media Server, the following information is required to order Media Servers. See Table 70, Equipment list: Media Server, on page 288.

**Table 70: Equipment list: Media Server**

| Media Server | | |
|---|---|---|
| Material Code: 170902 | Apparatus Code S8300 | Optional |
| Comcode (for Maintenance Ordering Only): | | |
| Comcode | Number of Items | Description |
| 108919994R | 1 | S8300 Media Server |
| The following field-replaceable component is contained in 108919994R: | | |
| 700246689R | 1 | S8300 Hard Drive |

# Avaya Cajun equipment

Use the information in Table 71, Avaya Cajun equipment, on page 289 when ordering Avaya Cajun equipment for use with the Avaya S8300 Media Server with G700 Media Gateway system.

**Table 71: Avaya Cajun equipment**

| Avaya Cajun Equipment | | |
|---|---|---|
| CASCADE/OCTAPLANE MODULE | | |
| Material Code: 108562943 | CAJUN MOD P330 STACKING | |
| | | |
| CASCADE CABLES | | |
| Material code: 108592445 | CAJUN P330 CABLE OCTAPLANE STACKING 1FT | |
| Material code: 108592437 | CAJUN P330 CABLE OCTAPLANE STACKING 6FT | |
| Material code: 108563453 | CAJUN CABLE ASSY X330RC REDUN STACKING | |
| | | |
| EXPANSION MODULES | | |
| Material code: 108562927 | CAJUN MOD P330 1000BSX UPLINK 2PT | The X330-S2 provides 1000Base-SX connectivity with two Multimode Fiber ports (up to 550 m,1804 ft) with LAG and Load Sharing |
| Material code: 108563032 | CAJUN MOD P330 1000BLX UPLINK 2PT | The X330-L2 provides 1000Base-LX connectivity with two Single Mode Fiber ports (up to 5 km,3.11 miles) with Link Aggregation (LAG) and Load Sharing |
| Material code: 108562992 | CAJUN MOD P330 1000BSX UPLINK 1PT | The X330-S1 provides 1000Base-SX connectivity with one Multimode Fiber port (up to 550 m,1804 ft) |
| Material code: 108562976 | CAJUN MOD P330 1000BLX UPLINK 1PT | The X330-L1 provides 1000Base-LX connectivity with one Single Mode Fiber port (up to 5 km,3.11 miles) |
| Material code: 108562968 | CAJUN MOD P330 10/100TX UPLINK 16PT | The X330-T16 adds 16 10/100Base-T ports. It allows up to 64 ports in a single switch and an impressive 640 per stack! Two LAGs can be created, with up to eight ports per group. |

*(1 of 2)*

**Table 71: Avaya Cajun equipment**

| Avaya Cajun Equipment | | |
|---|---|---|
| Material code: 108562950 | CAJUN MOD P330 100FX UPLINK 2PT | The X330-F2 adds two 100Base-FX ports which can be aggregated using LAG to provide a 200 Mbps link for backbone or high-speed server applications. |
| Material code: 108659178 | CAJUN P330 MOD EXP GBIC 2PT | The X330-G2 provides GBIC connectivity with an adapter for standard GBIC transceivers. |
| Material code: 108659194 | CAJUN MOD DUAL SPD OC12/0C3 SMF 15KM | |
| Material code: 108659186 | CAJUN MOD DUAL SPEED OC12 OC3 MMF 500M | |
| | | *(2 of 2)* |

## Replacing the G700 Media Gateway

Circumstances may require that the G700 Media Gateway be replaced, either because of hardware/firmware failure, or because of newer technology. Depending upon these circumstances, some or all of the components inserted into the G700 (S8300 Media Server, LED Panel, Avaya Expansion Module, Avaya Octaplane Module, or various Media Modules) can be reused in the replacement G700.

**NOTE:**
The procedures to replace an installed G700 Media Gateway with a new G700 are described in *Job Aid: Replacing the G700 Media Gateway, 555-245-752*. The G700 may or may not contain an S8300 Media Server, which can be configured as a primary controller or as a local survivable processor (LSP).

## Replacing the S8300 Media Server or hard drive

Circumstances may require that the S8300 Media Server or its hard drive be replaced, either because of hardware/firmware failure, or because of newer technology.

**NOTE:**
The term “S8300 hardware” is used to refer to either the S8300 Media Server circuit pack, including its hard drive, or to just the S8300 hard drive.

## Assumptions

The following items are assumed for the successful completion of this replacement procedure. If any of these assumptions do not apply to your scenario, some steps in the on-site replacement procedures may need to be modified:

- The existing S8300 hardware may or may not be functional.
- The S8300 may be configured as a primary controller or as an LSP.
- The following information is available:
  - customer FTP server IP address, login, and password
  - contents of a Pre-Installation Worksheet
- The technician is familiar with the connection and access methods to the S8300, including setting up a direct connection to the S8300 Services port and using the Maintenance Web interface.

**NOTE:**
See *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server, 555-234-100* for detailed information about setting up connections to the G700 and S8300 and the associated laptop configurations.

## Before you go to the site

There are seven possible scenarios for replacing the S8300 hardware, as summarized in Table 72, Replacement scenarios, on page 291. Each scenario requires a slightly different pre-installation preparation and a slightly different installation procedure. The different scenarios depend on:

- whether the original (currently installed) hardware is functional, and
- whether the software releases installed on the original and new hardware are the same, different, or unknown.

**Table 72: Replacement scenarios**

| Original hardware is: | Software release on hardware is: | Scenario | Replacement procedure |
|---|---|---|---|
| Functional | Original *earlier than* New | **1** | - Upgrade software on original hardware<br>- Back up data<br>- Replace hardware<br>- Install license and authentication files<br>- Configure network data<br>- Restore all data |
| | Original *same as* New | **2** | - Back up data<br>- Replace hardware<br>- Install license and authentication files<br>- Configure network data<br>- Restore all data |

***(1 of 2)***

**Table 72: Replacement scenarios**

| Original hardware is: | Software release on hardware is: | Scenario | Replacement procedure |
|---|---|---|---|
| | Original<br>*later than*<br>New | **3** | - Back up data<br>- Replace hardware<br>- Install license and authentication files<br>- Upgrade software on new hardware<br>- Configure network data<br>- Restore all data |
| Not Functional | Original<br>*earlier than*<br>New | **4** | - Replace hardware<br>- Install license and authentication files<br>- Use IW to configure server data<br>- Restore only translations & Audix announcements |
| | Original<br>*same as*<br>New | **5** | - Replace hardware<br>- Install license and authentication files<br>- Configure network data<br>- Restore all data |
| | Original<br>*later than*<br>New | **6** | - Replace hardware<br>- Install license and authentication files<br>- Upgrade software on new hardware<br>- Configure network data<br>- Restore all data |
| | Original SW release *unknown* | 7 | - Replace hardware<br>- Install license and authentication files<br>- Upgrade new hardware to latest bug-fix load, if needed<br>- Use IW to fully configure server data<br>- Restore only translations & Audix announcements |

*(2 of 2)*

You should determine which of the hardware replacement scenarios applies and obtain the needed information, software CDs, patches, and firmware files before going to the site.

When the S8300 hardware is replaced, you need to reconfigure the S8300 Media Server. The easiest way to do this is to back up the configuration data from the original hardware and do a full restore to the new hardware. This procedure will work only if the hardware that you back up from, and restore to, are running the same media server software release.

For scenarios **1**, **3**, and **6**, the original and new hardware are running different software releases. In these scenarios, you will need to do a software upgrade (on the original hardware for **1** and on the new hardware for **3** and **6**) to make the software releases the same. In scenario **6**, since the hardware is not functional, you cannot do a backup so you will restore the latest available backup. To do these upgrades, you will need to have a CD containing the appropriate media server software load. The software load will typically be the latest GA bug-fix load, but it could be an earlier load depending on what is required to make the software releases the same on the original and new hardware.

For scenarios **2** and **5**, the original and new hardware are running the same software release so no upgrades are required. For scenario **5**, you will restore the latest available backup.

For scenario **4**, you cannot use the latest available backup to restore the configuration data. (You cannot upgrade the original hardware or backup the configuration data because the hardware is not functional. You cannot do a full restore of the latest available backup because the original and new hardware have different software releases). In this scenario, you must do a full configuration using the Installation Wizard or the Maintenance Web Interface and restore just the translations and AUDIX files from the latest available backup.

For scenario **7**, you (and the customer) don't know the software release on the original hardware. You can't check the software release because the hardware is not functional. In this case, you must follow the replacement procedure in scenario **4**, with the additional step of upgrading the new hardware to the latest GA bug-fix load, if that load is not already installed on the new hardware. This upgrade step ensures that the system will not be downgraded in case the original hardware had the latest GA bug-fix load installed.

***Perform the following steps before going to the customer site:***

1. Download the current license file and authentication (password) file from the RFA website. The license file must be associated with the serial number of the G700 in which the defective hardware resides. Save the license and authentication files on the laptop that you will use at the customer site.
2. For scenarios **4** and **7 — i**f the original hardware is not functional, and the original hardware has an earlier (or unknown) software release than the release installed on the new hardware, then you need to do a full configuration (rather than a full restore).

   Create a pre-installation server worksheet, which will be used when configuring the S8300 after hardware replacement. There is an electronic version and a printable version of the pre-installation worksheet. The electronic version is used with the Installation Wizard to directly load the configuration data onto the S8300. The printable version is used to record the configuration data, which is then manually entered into the screens of the Installation Wizard or the Maintenance Web. The electronic version, used with the Installation Wizard, is recommended because it simplifies the data-entry task and is more accurate.

   You can obtain the pre-installation worksheet from http://support.avaya.com/avayaiw/.

   **NOTE:**
   You do not need to create a pre-installation worksheet for the other scenarios (**1**, **2**, **3**, **5**, and **6**).

3. For scenario **7** — if the software release on the original hardware is unknown, check to see if the software release on the new hardware is the latest GA bug-fix load. If not, obtain a CD with the latest GA bug-fix load.
4. Determine backup location, user name, ftp host name, directory, and password to do an FTP backup when on site. Keep this information handy for the restore.
5. For scenarios **1**, **3**, and **6** — if an upgrade is needed, obtain a CD with the appropriate release of the media server software to be used for upgrading the original or new hardware. (The appropriate release is whatever makes the releases on the original and new hardware the same after the upgrade).
6. For scenarios **1**, **2**, and **3**, obtain information about the customer's FTP backup server: IP address, user name, password, ftp host name, and directory.
7. Determine whether software patches will be needed and, if so, download the appropriate software patch to your laptop.
8. If the new hardware has a release of the media server software that is later than the release installed on the original hardware, you may need to upgrade the G700 firmware (See Upgrading firmware on page 355.

## At the customer site

Use the following procedure to replace the S8300 hard drive or the S8300 Media Server circuit pack (including its hard drive).

### *Procedure to replace the S8300 hardware*

1. If the S8300 hardware is still functional or can be made functional, connect your laptop to the Services port on the S8300 and access the Maintenance Web Interface.

   If you do not know whether the S8300 hardware is functional, perform the following procedure to determine if it is functional:

   **a** Connect your laptop (with a crossover cable) to the Services port on the S8300, open the IE browser, and connect to http://192.11.13.6.

   **b** If you do not get the Welcome screen, skip to Step e.

   **c** If you get the Welcome screen, click **Continue,** log in, and launch the Maintenance Web Interface.

   **d** Select **View Partition Status** under the "Server Configuration and Upgrades" category.

   — If the View Partition Status table, showing the status of the hda1 and hda6 partitions, the S8300 hardware is functional; skip to Step 2.

   — If the View Partition Status table is not displayed, or you get an error message, the S8300 hardware may not be functional; continue with Step e.

   **e** If the previous steps indicate that the S8300 hardware may not be functional, power-cycle the G700 (unplug and plug-in the power cord) and repeat Steps **a** - **d**. If you do not get the Welcome screen in Step **b** or if the View Partition Status table is not displayed in Step **d**, then the S8300 hardware is not functional — skip to Step 4.

   **NOTE:**
   If the S8300 hardware is not functional, skip Steps 2 and 3 and continue with Step 4.

2. Check to see if the new hardware has a higher software release than the current system. If so, upgrade the media server software on the original hardware to the same release as is on the new hardware. This applies to dot releases as well as major releases.

3. Back up data:

   **f** On the Maintenance Web Interface navigational panel, select **Backup Now** under the "Data Backup / Restore" heading.

   **g** On the Backup Now screen, check all of the following data sets:

   — **ACP Translations**; select the radio button for **Save ACP translations before backup**

   — **Server and System Files**

   — **Security Files**

   — If IA770 is installed on the S8300, also select **Audix Names, Translations and Messages**

**h** Select the **FTP** Backup Method and enter the customer-supplied information for:

— **User Name**

— **Password**

— **Host Name**

— **Directory**

**i** Click the **Start Backup** button.

**j** If IA770 is installed on the S8300, back up AUDIX announcements:

— Return to the **Backup Now** screen and uncheck all but **Audix Announcements**

— Select the FTP Backup Method and enter the login destination information as in Step 3-c.

— Click the **Start Backup** button.

**4** Install the new hard drive or S8300 Media Server.

**CAUTION:**
Be sure to wear a properly grounded ESD wrist strap when handling the S8300 Media Server, hard drive, and the (optional) 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.

**a** Shutdown the S8300 Media Server using either the Web interface or the manual Shutdown button on the S8300 faceplate.

— On the Maintenance Web Interface, select **Shutdown this Server** under the "Server" heading. Select the **Delayed** option, leave the "After Shutdown, Restart System" unchecked, and click **Shutdown**.

— Alternatively, you can manually initiate a shutdown by pressing the Shutdown button on the S8300 faceplate. Hold the button in until the green "OK to Remove" LED starts blinking.

In either case, when the "OK to Remove" LED goes on steady, you can power-down the G700. If the LED does not go on steady within 5 minutes, proceed to the power-down step.

**b** Power-down the G700 by unplugging the power cord.

**c** Loosen the two thumb screws on the S8300.

**NOTE:**
When removing or inserting the S8300 circuit pack, the LED module (above slot V1) must also be removed or inserted together with the S8300.

**d** Disengage the LED module and the S8300 circuit pack and remove them together from the G700.

**NOTE:**
If you are replacing only the hard drive (and keeping the S8300 circuit pack), continue with Step e. If you are replacing the entire S8300 Media Server (including its hard drive), skip to Step 1.

**e** Unscrew the four screws on the bottom of the S8300 circuit pack that attach to the hard-drive standoffs (Refer to Figure 83, S8300 hard drive replacement, *on page 298*).

**f** Detach the hard-drive ribbon cable from the hard drive (leave cable attached to the S8300 circuit pack).

**g** Unpack and install the new hard drive on the S8300. Standoffs for the new hard drive should be included in the new hard drive package.

**NOTE:**
If standoffs are not included with the new hard drive, remove the standoffs from the old drive and reuse them. ***Before screwing the standoffs into the new hard drive, clean the threads thoroughly with a damp cloth or paper towel***.

**h** Screw the standoffs into the new hard drive.

**CAUTION:**
*In* Step i*, 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 83, S8300 hard drive replacement, on page 298*.

**i** Connect the open end of the hard-drive ribbon cable (which is attached to the S8300 circuit pack) to the replacement hard drive, as shown in Figure 83, S8300 hard drive replacement, *on page 298*. Connect pin number one to the end of the ribbon connector marked with the red stripe.

**j** Place the hard drive on the S8300 circuit pack with the standoffs aligned with the screw holes.

**k** Hold the S8300 circuit pack on its side, with the hard drive in place, and screw the four screws through the bottom of the S8300 circuit pack into the hard-drive standoffs.

**l** If you are replacing the S8300 circuit pack, and if the CWY1 board is installed on the original S8300, remove the CWY1 board from the original S8300 and install it on the new S8300 circuit pack.

**m** Insert the S8300 into slot V1 of the G700. The LED panel (above slot V1) must be removed and reinserted together with the S8300 circuit pack. Insert both the LED panel and S8300 circuit pack about 1/3 of the way into the guides (the guides are in slot V1 for the S8300 and above slot V1 for the LED panel). Push both circuit packs (together) back into the guides, gently and firmly, until the front of each circuit pack aligns with the front of the G700.

**n** Secure the S8300 faceplate with the thumb screws. Tighten the thumb screws with a screw driver.

**5** Power up the G700 by plugging in the G700 power cord.

**6** Connect your laptop to the Services port on the S8300 and access the Maintenance Web Interface.

**7** Enable FTP on the S8300:

**a** On the Maintenance Web Interface, select **Enable/Disable Anonymous FTP** under the “Security heading

**b** Click on **Enable**

**8** Install the License and Authentication files.

**9** If necessary, upgrade the media server software on the new hardware:

- **a** If the software release installed on the new hardware is earlier than the release on the original hardware, upgrade the software on the new hardware to match the release on the original hardware.
- **a** If the software release on the original hardware is unknown, and the software on the new hardware is not the latest bug-fix load, upgrade the software on the new hardware to the latest bug-fix load.

**10** Configure the S8300 and restore data. Do either Step a or Step b:

- **a** If the original hardware is functional ***or*** if the software release installed on the original hardware is the ***same as*** or ***later than*** the release installed on the new hardware, then:
  - — Configure the network data (Host Name, IP address, subnet mask, default gateway IP address).
  - — Restore all data
- **b** If the original hardware is ***not*** functional ***and*** the software release installed on the original hardware is either ***unknown or earlier than*** the release installed on the new hardware, then:
  - — Configure the S8300 as you would a new install using either the Avaya Installation Wizard and the Pre-Installation Worksheet previously created, or using the Maintenance Web Interface.
  - — Restore only the translations and the Audix announcements

**11** If the new hardware has a later software release than the original hardware, check to see if you need to upgrade the G700 firmware as described in Step 8 in the Before you go to the site section.

**12** Install any software patches required.

**13** Check for and resolve any new alarms.

**14** Test as appropriate — for example, make station and trunk calls.

**15** Save translations. If the S8300 on which you replaced the hardware is configured as an LSP, save translations on the primary controller, not the LSP.

**16** Disable FTP on the S8300:

- **a** On the Maintenance Web Interface, select **Enable/Disable Anonymous FTP** under the “Security” heading
- **b** Click on **Disable**

**Figure 83: S8300 hard drive replacement**

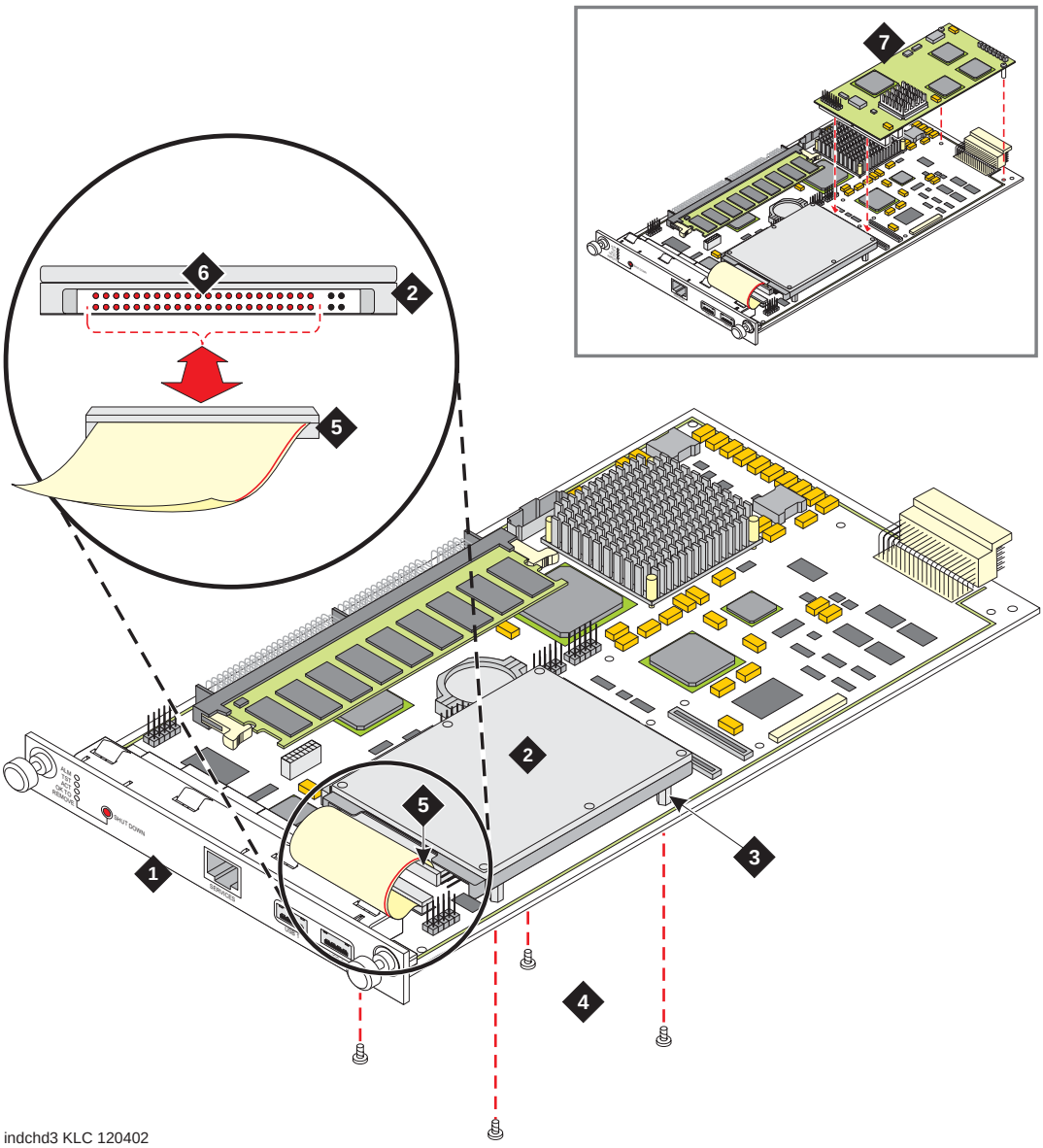



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | S8300 circuit pack | **5** | Ribbon-cable connector |
| **2** | Hard drive | **6** | Hard-drive connector pins |
| **3** | Hard-Drive standoffs | **7** | Optional CWY1 board |
| **4** | Screws | | |

# Replacing Media Modules

The information in the Table 73, Equipment list: Media Modules, on page 299 is necessary when ordering or replacing Avaya Media Modules.

**Table 73: Equipment list: Media Modules**

| Media Modules | | |
|---|---|---|
| T1/E1 Media Module | | |
| Material Code: 170900 | Apparatus Code: MM710 | Optional |
| ComCode (for Maintenance Ordering Only): 700221161R | | |
| DEF DS1 LOOPBACK JACK 700A | | |
| Provides the ability to remotely trouble shoot the T1/E1 Media Module. It is required for any customer with a maintenance contract and highly recommended for any other customer. | | |
| Material Code: 107988867R | Apparatus Code: None | Required for any customer with a maintenance contract and a T1/E1 Media Module, highly recommend for other customers to avoid expensive technician visit. |
| VoIP Media Module | | |
| Material Code: 170901 | Apparatus Code: MM760 | Optional |
| ComCode (for Maintenance Ordering Only): 700221179R | | |
| DCP Media Module | | |
| Material Code: 170898 | Apparatus Code: MM712 | Optional |
| ComCode (for Maintenance Ordering Only): 700221153R | | |
| | BRI Media Module | |
| Material Code: 170898 | Apparatus Code: MM720 | Optional |
| ComCode (for Maintenance Ordering Only): 700221138R | | |
| Analog Station/Trunk Media Module | | |
| Material Code: 170899 | Apparatus Code: MM711 | Optional |
| ComCode (for Maintenance Ordering Only): 700221146R | | |

Reasons for replacing a Media Module include:

- Repairing a damaged Media Module
- Changing Media Module type

The modules on the G700 are not inserted until the G700 registers with Communication Manager. Likewise, all Media Modules and associated Maintenance Objects are removed if the G700 link goes down. 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 the Media Modules is detected. Listings of the G700 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 G700 Media Gateway, where board type, suffix, and vintage are verified. The G700 then sends appropriate H.248 messages to the controller, thus creating Communication Manager objects.

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

**WARNING:**
The G700 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.

### *Replacing Avaya Media Modules*

1. Identify and mark all cables.
2. Undo the cables.
3. Undo the captive screws and slide out the old Media Module.
4. Position the Media Module squarely before the selected slot on the front of the G700 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 84, Inserting Media Modules, on page 301)
6. Apply firm pressure to engage the connectors.

   The Media Module connector has different length pins. The long pins will engage first to provide grounding. Medium length and short pins will provide power and signal.

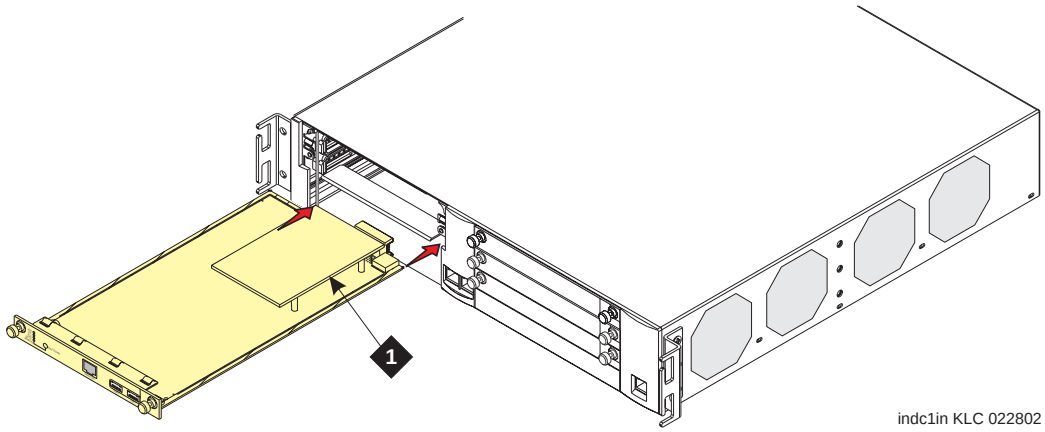
7 Lock the Media Module into the chassis by tightening the spring-loaded captive screws on the front of the module.

8 Plug in the cables in the correct order.

**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 84: Inserting Media Modules**




## Replacing Avaya Expansion Modules

The Avaya Expansion Modules provide vastly increased networking and connectivity capabilities. For a complete description of the Avaya Expansion Modules, see *Avaya P330 Manager User Guide*. These modules may be mounted in the G700 in the Expansion Module slot on the left side of the faceplate. The G700 must be powered off before you insert or remove an Avaya Expansion Module.

**WARNING:**

The G700 must not be operated with any slot open; empty slots must be covered with the supplied blank plates.

**CAUTION:**

The G700 must be powered off before you insert or remove an Avaya Expansion Module.

### *Replacing an Expansion Module in the G700*

1 Power off the unit if the equipment has been in operation.

2 Identify and mark all cables.

3 Undo the cables.

4 Remove the blank plate covering the slot.

5 Align the printed circuit board with the interior guide rails.

**NOTE:**
Note: The printed circuit board fits into the guide rail. The metal base plate does not.

6 Firmly press the Expansion Module until it is completely inserted into the G700.

7 Tighten the two screws on the front panel of the Expansion Module.

**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.

## Replacing an Avaya Octaplane Stacking Module

G700 Media Gateways can be mounted in equipment stacks with routers, switches, or other G700s. The stack is limited to ten elements. To link multiple units, each G700 must be equipped with an Avaya Octaplane Stacking Module, which is mounted through the rear panel of the G700. See *Hardware Guide for Avaya Communication Manager, 555-233-200* for a general description of the hardware.

### Insert an Avaya Octaplane Stacking Sub-Module

1 Undo the cables.

2 Remove the blank plate from the back of the G700.

3 Insert the Avaya Octaplane Stacking Sub-Module gently in the slot, ensuring that the metal base plate is aligned with the guide rails.

4 Press the Avaya Octaplane Stacking Sub-Module in firmly until the connector at the back of the module is completely inserted into the internal connector on the G700.

5 Tighten the screws on either side of the module.

# S8500 component maintenance

This section contains procedures for the following equipment:

- Replacing the S8500 hard drive on page 303
- Replacing the S8500 Media Server on page 303
- Replacing the Remote Supervisor Adapter (RSA) on page 304
- Replacing the Remote Supervisor Adapter (RSA) on page 304

## Replacing the S8500 hard drive

For procedures to replace the S8500 hard drive, see *Job Aid: Replacing the S8500 Hard Drive, 555-245-761*.

## Replacing the S8500 Media Server

For procedures to replace the S8500 Media Server, see *Job Aid: Replacing the S8500 Media Server, 555-245-762*.

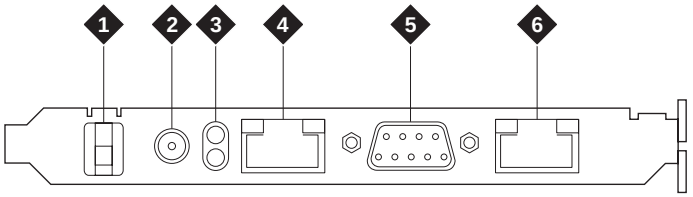
# Replacing the Remote Supervisor Adapter (RSA)

This section contains information and procedures for replacing the Remote Supervisor Adapter (RSA) board in the Avaya S8500 Media Server. Detailed discussions of these topics follow:



The RSA is factory installed in PCI-X slot 1 of the S8500 Media Server. Figure 85, RSA faceplate and connectors, on page 304 shows the RSA faceplate and connectors.

**Figure 85: RSA faceplate and connectors**




h3msrsap LAO 071503

**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Power retaining clip | **4** | ASM RS-485 connector |
| **2** | External power supply connector | **5** | RS-232 serial connector |
| **3** | Power and error LEDs | **6** | Ethernet connector |

**CAUTION:**
Wear an antistatic wrist ground strap whenever handling the media server or media server components. Connect the strap to an approved ground, such as an unpainted metal surface.

## Backing up the RSA

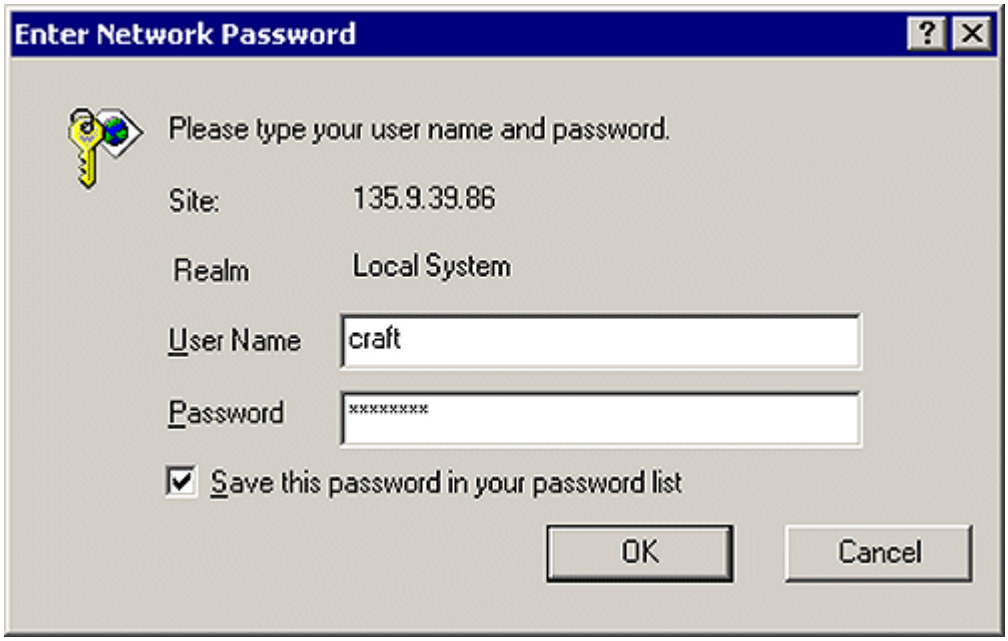
Backup the RSA configuration before shutting down the S8500 Media Server. If it is not possible to backup the RSA at this time, locate the most recent RSA backup file before proceeding.

Complete the following steps to backup the RSA configuration:

1. Establish a connection from the services laptop to the RSA:
   - Direct connect through a crossover cable from the laptop to the Ethernet port on the RSA
   - Other network connection
2. Open a internet browser window.
3. In the address field of the browser, type the IP address for the RSA and press **Enter**.

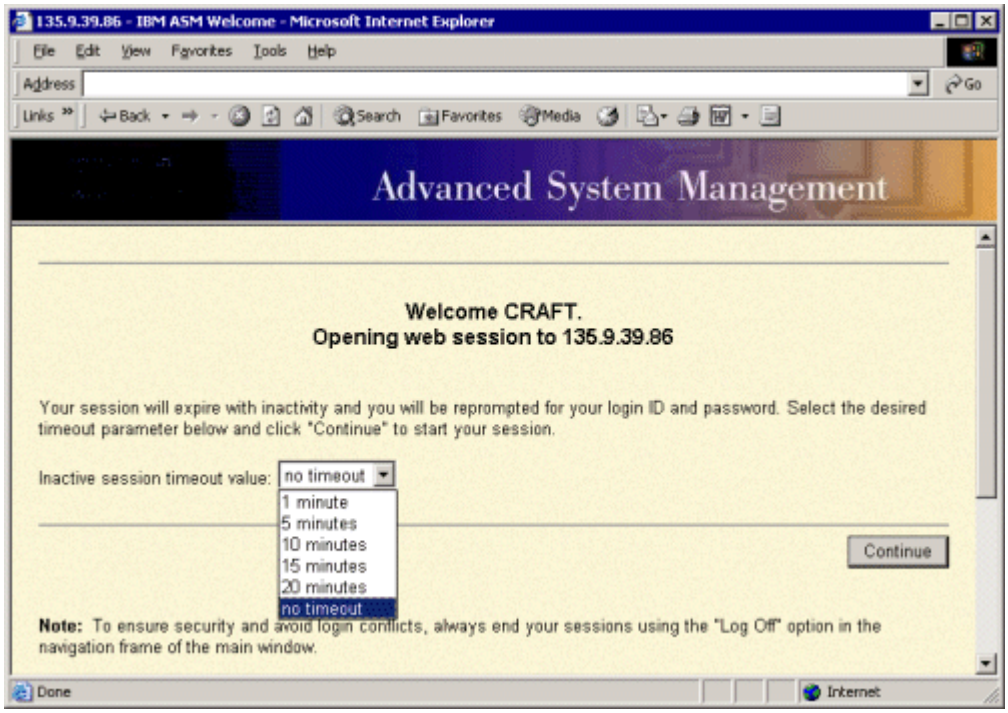
   The ***Enter Network Password*** window appears (Figure 86, Enter Network Password window, on page 305).

**Figure 86: Enter Network Password window**




4. In the **Enter Network Password** window, enter the default login of **craft** and the unique password for the RSA assigned to this location. The password can be obtained from the Automatic Registration Tool (ART) website.
5. In the RSA welcome window, select the **no timeout** value from the drop-down list. The **no timeou**t value allows 60 minutes of use before disconnecting. See Figure 87, RSA Welcome window, on page 306 for an example of the welcome window.

**Figure 87: RSA Welcome window**



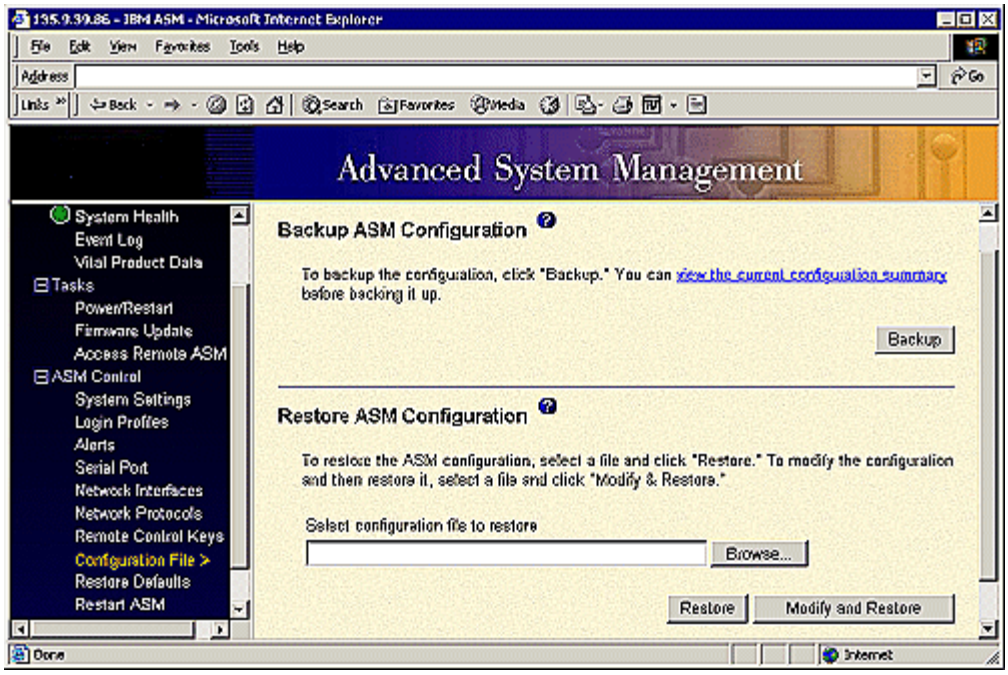

**NOTE:**
If the session times out unexpectedly, click **Start New Session** and **Refresh**.

6 Click **Continue** to start the session.

7 Click **Configuration File** in the navigation pane.

8 In the **Backup ASM Configuration** section click, **view the current configuration summary**.

**Figure 88: Backing up the ASM configuration**




9 After verifying that the current configuration summary settings are correct, click **Close**.

Now you can see the ***Backup ASM Configuration*** window (Figure 88, Backing up the ASM configuration, on page 307).

10 In the **Backup ASM Configuration** section click **Backup**.

11 Enter a name for the backup fileset and choose a location to write the backup files.

12 Click on one:

- For Windows Internet Explorer: Select **Save this file to disk** and then **OK**.
- For Netscape Navigator: Select **Save File**.

## Backing up the Media Server

Before replacing the RSA card, the media server is powered down and all power connection removed. As a security measure, backup the media server before powering it down.

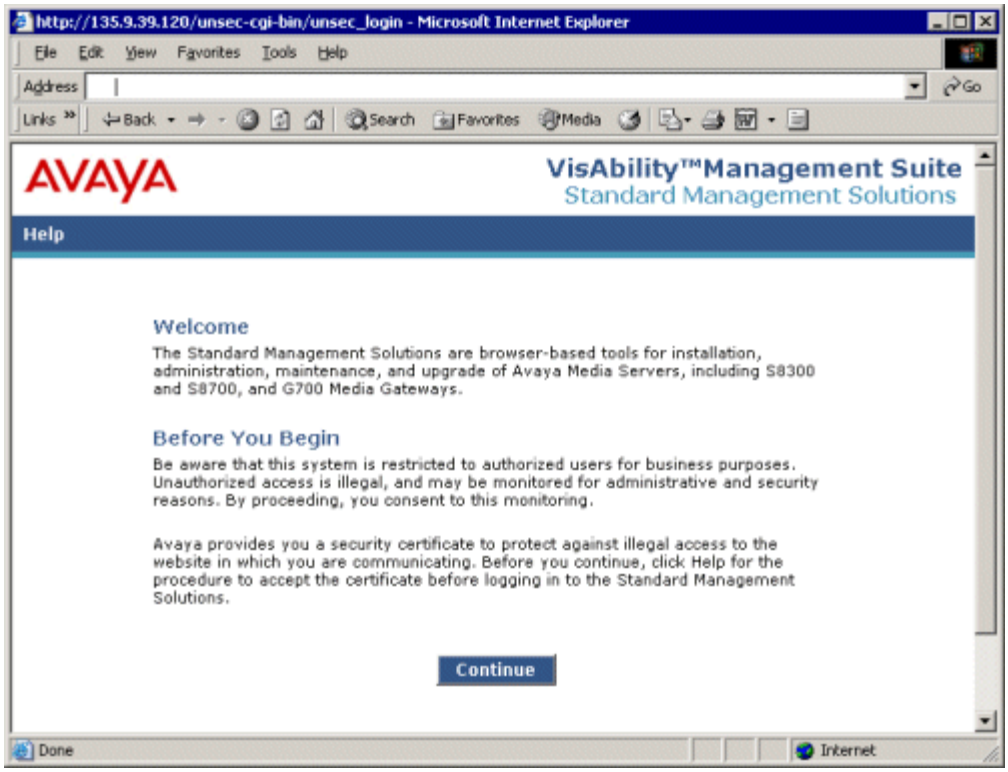
1 Connect the laptop to the port labeled 2 (Eth 1) on the back of the media server using the crossover cable.

2 Open a browser window on the laptop.

3 In the Address field of the browser, type in the URL for the media server and press **Enter**.

A welcome window opens (Figure 89, Figure 5: Sever Welcome window, on page 308).

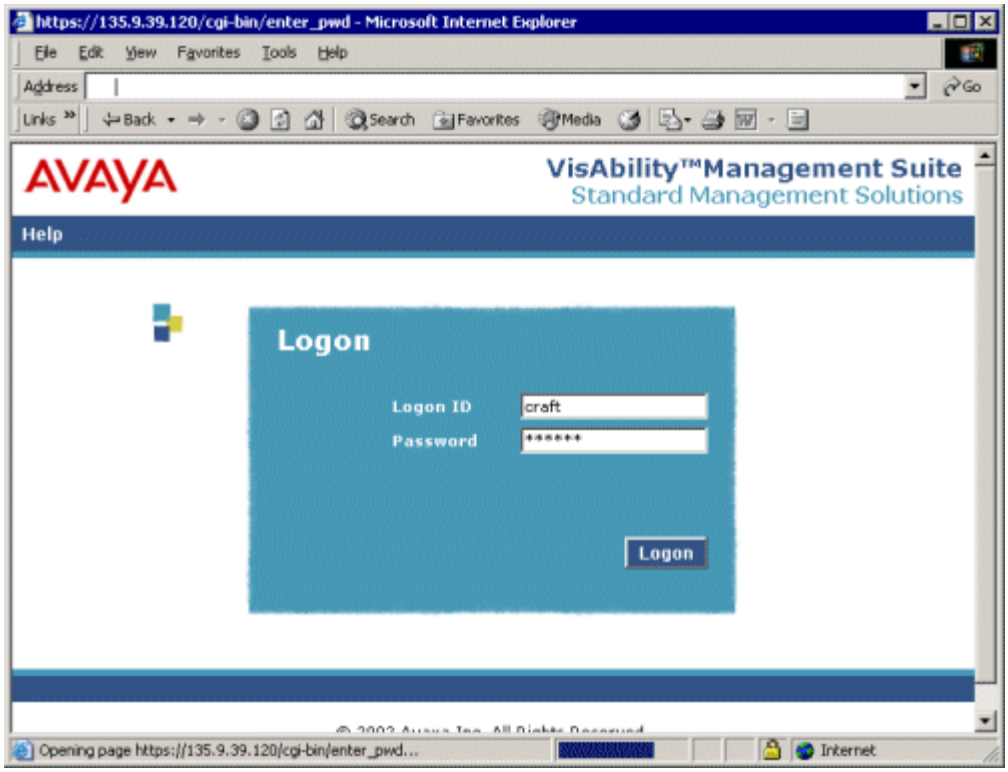
**Figure 89: Figure 5: Sever Welcome window**




4 Accept the Avaya certificate by clicking **Yes**.

5 Log into the media server using the **craft** logon and the associated password (Figure 90, Logon window, on page 309).

**Figure 90: Logon window**




6 Suppress alarm origination by clicking **Yes**.

7 Click **Launch Maintenance Web Interface.**

8 Click **Backup Now** in the navigation pane.

9 Select all data sets under the **Data Sets** heading.

10 Select one of the following backup methods:

- FTP
- Email
- Local PC card

11 If you want to encrypt the backup, select the **Encrypt backup using pass phrase** check box and enter a phrase in the box.

12 Click **Start Backup**.

## Powering down the Media Server and RSA

After the backup is finished, complete the following steps to power down the media server and the RSA.

1 From the media server Web interface click **Shutdown Server**.

2 Select **Delayed Shutdown**.

3 Click **Shutdown**.

4 After the media server shuts down, unplug the power cord from the back of the server.

5 Unplug the external power supply connection (Note 2 in Figure 85, RSA faceplate and connectors, on page 304) from the RSA.

**DANGER:**
**Ensure that all power is removed from the media server and the RSA.**

6 Disconnect the modem from the RS-232 port on the RSA.

7 Disconnect and label the LAN connection (if used) from the Ethernet port on the RSA.

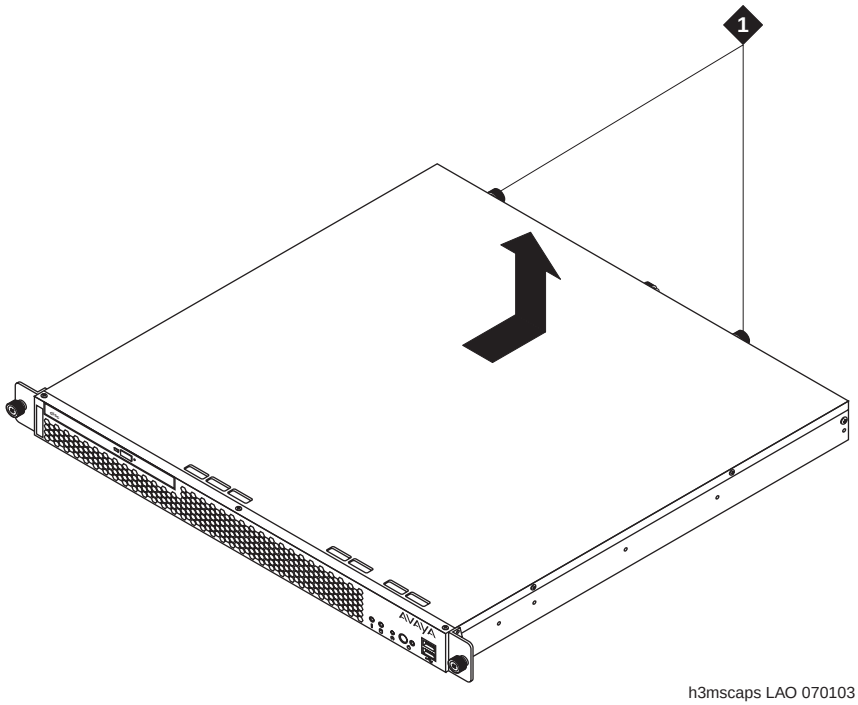
8 Pull the server forward so that the server rails expand and the retaining clips on the rails click into place.

## Removing the cover of the Media Server

Complete the following steps to remove the cover of the Media Server:

1 Unscrew the two captive screws on the back of the media server, as shown in Figure 91, Captive screws, on page 310.

**Figure 91: Captive screws**




h3mscaps LAO 070103

**Figure notes**

1 Captive screws

2 Slide the server cover back from the front panel until the cover's tabs are released from the top slot of the front panel.

3 Lift the cover straight up and move it away from the server.

## Replacing the ribbon cable

The 20-pin ribbon cable connects the RSA to the server system board and is required for power and data transfer. The ribbon cable is shipped in the same box as the RSA. Replace the ribbon cable before installing the new RSA card.

Complete the following steps to remove and replace the ribbon cable:

1. Remove one side of the ribbon cable from the system-management connector on the system board (CN-12) and the other side from the system-management connector on the RSA.
2. Connect one side of the new ribbon cable to J44 on the system board. You will install the other side of the ribbon cable to the new RSA (see Step 3 in the procedure titled, Installing the new RSA card on page 312).

## Removing the adapter support bracket and riser connector

The RSA card resides in PCI-X slot 1 located under the adapter support bracket. Remove the adapter support bracket and the riser connector together by performing the following steps:

1. Loosen the captive screw located to the right of the slot labeled PCI 1.
2. The riser connector must be removed by pulling straight up on the adapter support bracket. Place one finger under the screw on the far end of the riser connector and one finger under the adapter support bracket near the captive screw and pull straight up, as shown in Figure 92, Removing the RSA from the riser connector, on page 312.

**Figure 92: Removing the RSA from the riser connector**

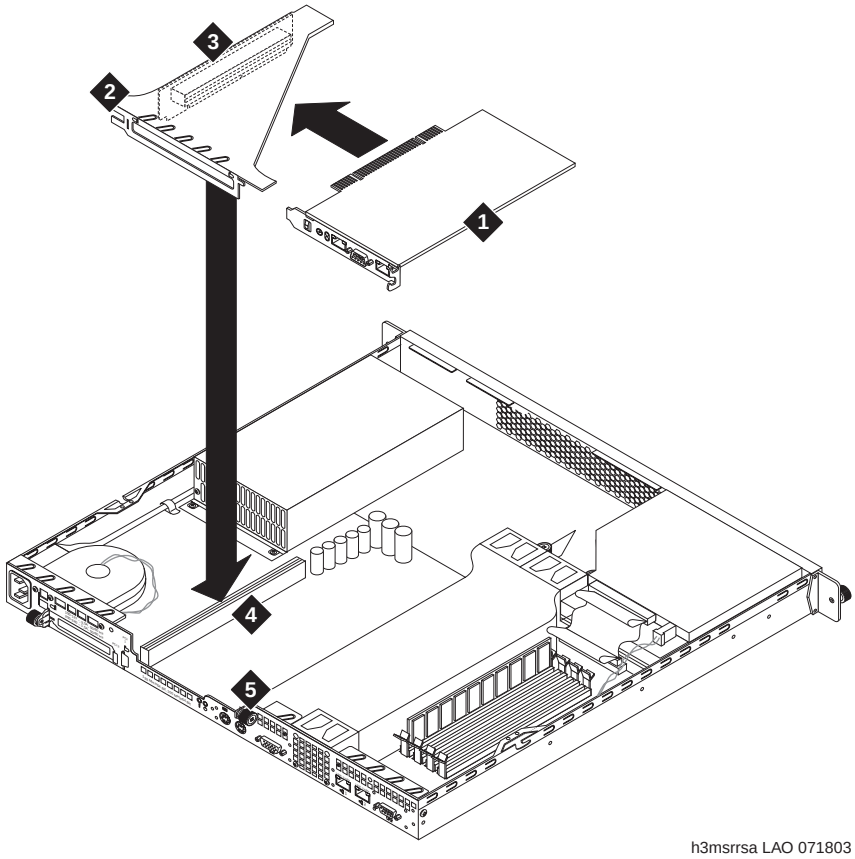



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | RSA | **4** | Connector |
| **2** | Adapter support bracket | **5** | Captive screw |
| **3** | Riser card connector | | |

**3** Remove the RSA card from PCI-X slot 1 by pulling the card gently out of the riser card connector.

## Installing the new RSA card

**1** Touch the static-protective package containing the adapter to any unpainted mental surface of the S8500 Media Server. Then remove the RSA card from the static-protective package. Avoid touching the components and gold-edge connectors on the RSA card.

**2** Carefully grasp the RSA by the top edges or upper comers, component side facing up, and align it with the PCI-X slot one opening. Press the RSA firmly into the riser card connector.

**CAUTION:**
Make sure the RSA card is completely and correctly seated in the riser card connector before you turn on the S8500 Media Server. Incomplete insertion might cause damage to the system board or RSA card.

**3** Connect the ribbon cable to the system-management connector located on the back on the card.

4 Replace the adapter support bracket lining up the tabs on each side of the bracket and the screw holes on the riser card connector.

5 Align the riser card with the connector and the tabs on the adapter support bracket with the provided holes and press the riser card firmly into the connector.

6 Tighten the captive screw to the right of the slot.

**NOTE:**
Route the ribbon cable so that it does not block the flow of air from the fans.

## Replacing the cover of the Media Server

1 Replace the cover onto the server.

2 Slide the cover forward so the cover's tabs slide into place under the top slots of the front panel.

3 Finger-tighten the thumb screws on the back of the server.

4 Release the retaining tabs on the rails and slide the S8500 Media Server back into place on the data rack.

## Connecting the cables to the RSA

1 Connect the external power supply (Note 2 in Figure 85, RSA faceplate and connectors, on page 304) to the RSA.

**NOTE:**
Do not apply power to the media server yet.

2 Connect the modem to the RS-232 port.

3 Do not plug in the LAN connection (if used). You will need to access the Ethernet port on the RSA once power is restored.

## Powering up the Media Server

Complete the following steps if you want to start the server at this time:

1. Plug the power cord in the back of the server.
2. Press the Power Button located on the front on the right hand side.
3. Log into the server to ensure that the startup is complete.

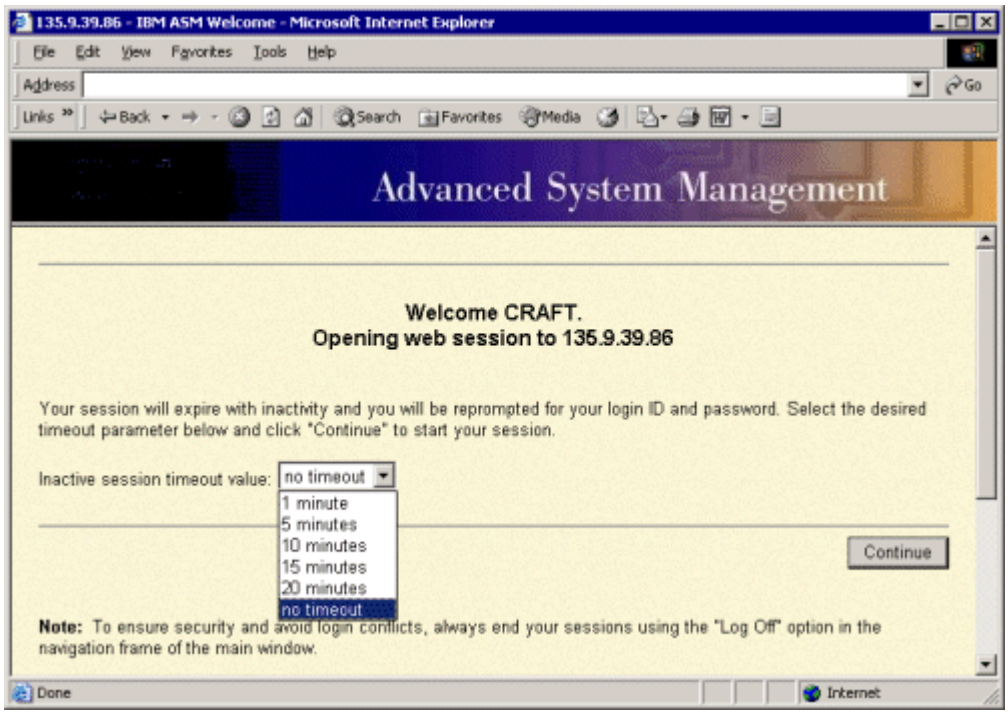
## Restoring the RSA configuration

Complete the following steps to restore the RSA configuration information:

1. Connect the services laptop to the Ethernet port on the RSA using a crossover cable.
2. Open a browser window.
3. Type **192.11.13.6** in the address field of the browser, and press **Enter**.

   The ***Enter Network Password*** window appears.
4. In the **Enter Network Password** window, enter the default login of **craft** and default password of **passw0rd** (with a zero).
5. In the RSA welcome screen, select the no timeout value from the drop-down list (see Figure 93, RSA Welcome screen, on page 314). The no timeout value allows 60 minutes of use before disconnecting.

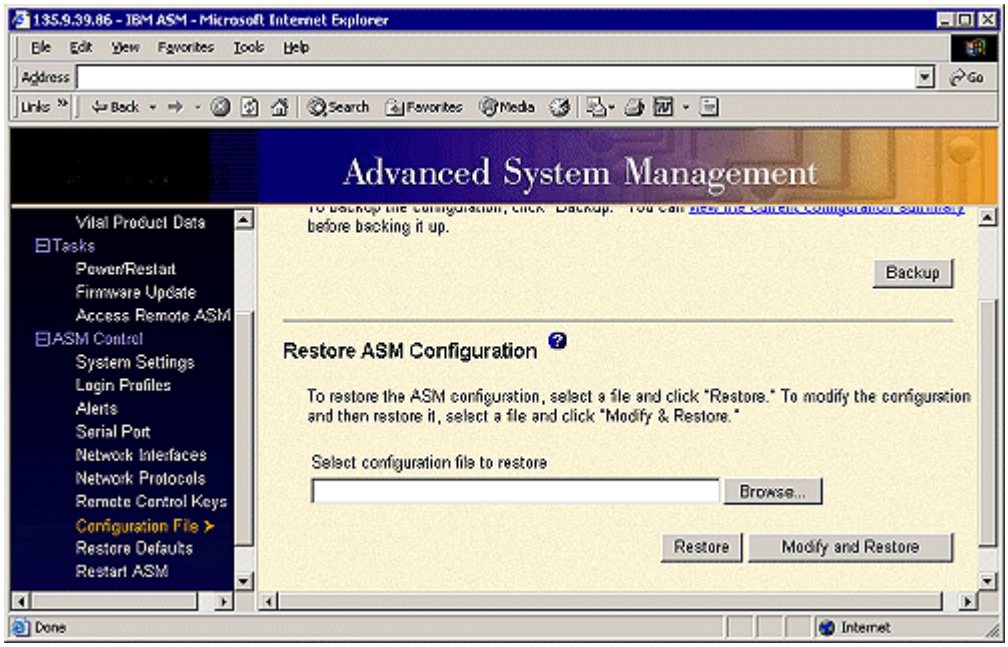
**Figure 93: RSA Welcome screen**




6. Click **Continue**.
7. Click **Configuration File** in the navigation pane.

8 In the **Restore ASM Configuration** section, click **Browse**. See Figure 94, Restoring ASM configuration, on page 315 for an example of the restoring ASM configuration window.

**Figure 94: Restoring ASM configuration**




9 Click the saved configuration file that you want to restore and click **Open**.

The file will appear in the box.

10 Click **Restore Configuration**. A progress window shows the status of the restore.

A confirmation window opens when the update is completed.

11 Click **OK** to restart the RSA.

12 Click **OK** to close the current browser window.

## Upgrading the RSA firmware

After installing the new RSA board, you must ensure that its firmware version is compatible with the release of Communication Manager running on the S8500 Media Server. This might involve upgrading the RSA firmware to the latest version. Before that you must first use these two procedures:

- Checking the firmware version on the new RSA on page 315
- Checking for the compatible firmware version on page 316

### *Checking the firmware version on the new RSA*

To check the version of firmware on the new RSA

1 Log into the RSA card through a browser window.

2 Select **Server > Monitors > System Health > Vital Product Data**.

3 At the bottom of the report the Advanced System Management (ASD) Vital Product Data (VPD) shows the Build ID.

4 Also check the readme.txt file for the Version and Revision numbers.

**NOTE:**
If you have root permission, establish a command line interface (CLI) connection and type **getvpd** to obtain the Vital Product Data report.

### *Checking for the compatible firmware version*

To check what RSA firmware version is compatible with the release of Communication Manager that is running on the server:

1 Open an browser window on your laptop.

2 Enter www.support.avaya.com in the address field.

3 Highlight **Support** in the top heading.

4 Highlight and click **Software and Firmware Downloads**.

5 Click **RSA** in the left pane.

6 Check **See All Releases**

7 Select the Communication Manager release running on the media server.

8 Compare the firmware version listed with the version on the new RSA board.

If the new RSA firmware is compatible, complete the section.

### *Upgrading the RSA firmware*

Use this procedure to upgrade the RSA firmware:

1 On your laptop, click on the required version of RSA firmware.

2 A download window opens. Click **Save**.

A ***Save As*** window opens.

3 Choose the location to save and file and a file name. Click **Save**.

A confirmation window opens when the transfer is complete.

**NOTE:**
The RSA firmware is loaded into the RSA card as three separate files. So, either there will be three files on the support site, or the user will download a single file and split it into the three separate files with WinZip or a similar program.

4 Log into the RSA using the instructions found under the Backing up the RSA on page 305.

5 In the navigation pane, select **Firmware Update**.

6 In the **Choose File** window, click **Browse**. Go to the saved location from Step 3.

7 Click on one of the three firmware files and then click **Open**.

The file name appears in the box next to **Browse**.

8 Click **Update** to begin the firmware update.

A progress window opens as the files are transferring to temporary storage on the RSA.

A confirmation window opens when the transfer is complete.

9 Verify that the file in the confirmation window is the file you want to update. If you do not want to continue click **Cancel**.

10 To continue with the firmware update click **Continue**.

A progress window opens as the firmware on the RSA updates. A confirmation window appears when the update is completed.

11 Repeat Step 6 through Step 9 for the remaining two firmware files.

12 Restart the RSA by clicking on **Restart**.

13 Click **OK** to continue.

14 Click **OK** to close the browser window.

15 Log into the RSA.

## Checking the RSA installation

Check the following to ensure that the installation was successful:

1 Under **Monitors, System Health** ensure that the RSA can read the system health of the S8500.

If the RSA cannot read the system health of the S8500:

- The RSA may not be seated correctly in the riser card. Follow the instruction starting at Powering down the Media Server and RSA on page 309 to reseat the RSA.
- The RSA may be defective.
- The S8500 Media Server may be defective. Contact the TSO for verification and instructions.
- The ribbon cable might not be seated at either or both ends.

2 Under **ASM Control, Login Profiles** verify that the login information was restored.

If the login information is not correct:

**a** Restore the configuration information file again (Restoring the RSA configuration on page 314).

*or*

**b** Manually input the correct information.

3 Under **ASM Control, Alerts** verify that the remote alert recipients are correct.

If the alert information is not correct:

**a** Restore the configuration information file again (Restoring the RSA configuration on page 314) or manually input the correct information.

**b** Generate an alarm to a test alarm by clicking **Generate Test Alert**. If the RSA has LAN connectivity, send an SNMP alert. Call the Avaya alarming group and verify the alarm was received.

- Under **Monitors, Event Log** ensure that there are no errors (red X) listed in the log.

If an error exists:

**a** Check the timestamp of the error.

**b** If the error occurred after you replaced the RSA, contact the TSO for further instructions.

## Restoring the RSA defaults

**CAUTION:**

***DO NOT*** select **Restore Defaults**. Doing so removes the Avaya defaults that are superimposed over the manufacturers' resulting in loss of access to the RSA card. "Restore" in this instance means reinstating the manufacturer's factory default settings and rendering the server incapable of providing IP Telephony.

Avaya defaults can be restored manually or by restoring the Avaya default file:

- To manually restore the default file use the steps outlined in the Configuration File section of the *Installing the S8500 Media Server with the G650 Media Gateway, 555-245-107*.
- To restore the Avaya default file go to http://support.avaya.com or look for the file on the Communication Manager 2.0 CD for Linux Servers and Gateways.

# Replacing the S8500 dual network interface

This section describes the steps required to replace an existing dual network interface card (NIC) on the S8500 Media Server. The control network traffic from the server out to the dedicated customer LAN travels through the NIC. The components of this procedure include:

- Backing up the Media Server on page 319
- Powering down the Media Server on page 321
- Removing the fan unit on page 323
- Removing the old NIC on page 323
- Inserting the new NIC on page 324
- Replacing the fan unit on page 325
- Replacing the cover and cabling on page 325
- Powering up the server on page 326
- Checking LED activity on the dual NIC on page 326
- Confirming original Ethernet configuration on page 326

**CAUTION:**
Wear an antistatic wrist ground strap whenever handling the media server or its components. Connect the strap to an approved ground, such as an unpainted metal surface.

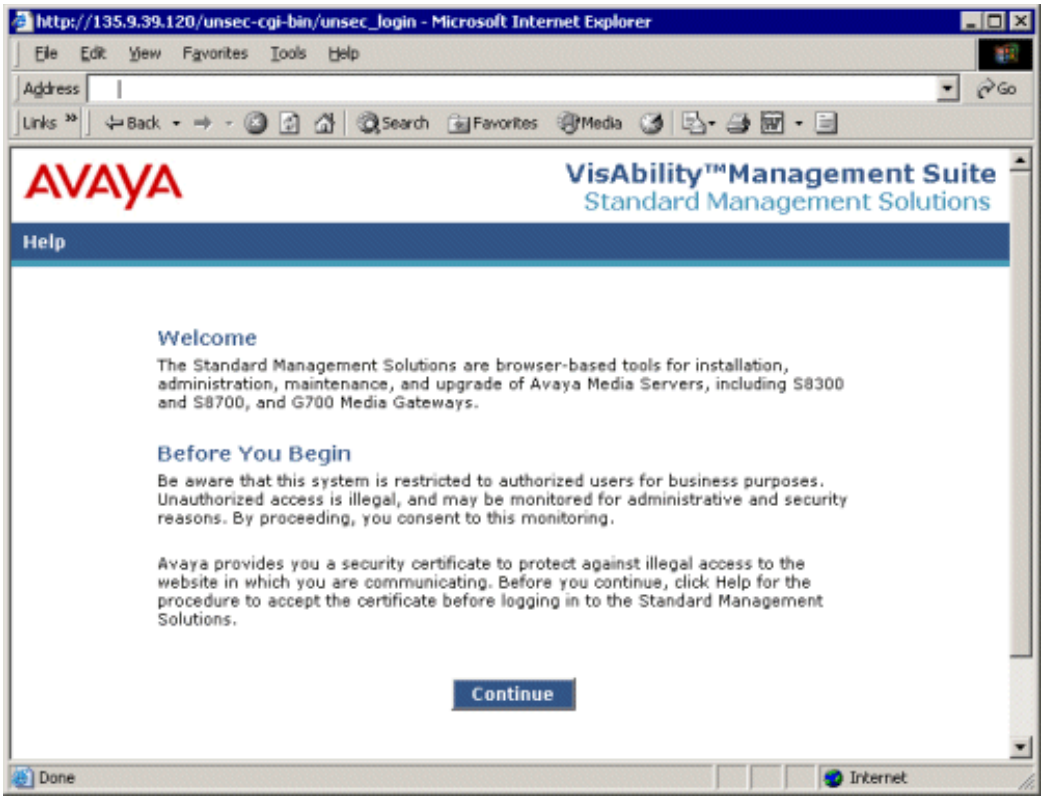
## Backing up the Media Server

Backup the media server before you power it down. To backup the media server complete the following steps:

1. Connect the services laptop to the port labeled 2 (Eth 1) on the back of the media server using the crossover cable.
2. Open a browser window on the laptop.
3. In the address field of the browser, type in the URL for the media server and press **Enter**.

   A welcome window opens (Figure 95, Welcome Window, on page 320).

**Figure 95: Welcome Window**



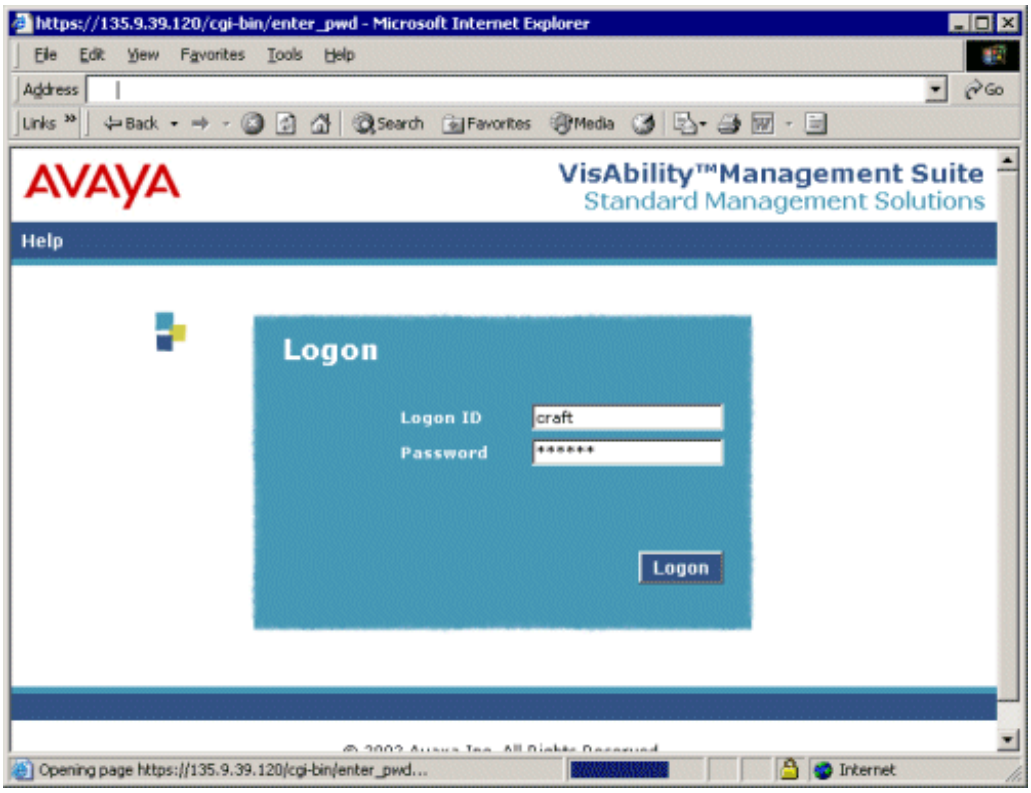

4 Click **Continue**.

5 Accept the Avaya certificate by clicking **Yes**.

The logon window appears (Figure 96, Logon window, on page 321).

6 Type **craft** in the `Logon ID` field and the password (obtained from ART) in the `Password` field () and click **Logon**.

**Figure 96: Logon window**




7 Suppress alarm origination by clicking **Yes**.

8 Click **Launch Maintenance Web Interface**.

9 Click **Backup Now** in the navigation pane.

10 Select **all data sets** under the **Data Sets** heading.

11 Select one of the following backup methods:

- FTP
- E-mail
- Local PC card

12 If you want to encrypt the backup, select the **Encrypt backup using pass phrase** check box and type a pass phrase.

13 Click **Start Backup**.

## Powering down the Media Server

After the backup is finished, complete the following steps to power down the media server.

1 From the media server Web interface click **Shutdown This Server**. Select **Delayed**.

2 After the media server shuts down unplug the power cord from the back of the server.

3 Unplug the power cord from the RSA.

4 Disconnect the modem from the RS-232 port on the RSA.

5 Disconnect and label the LAN connection (if used) from the Ethernet port on the RSA.

6 Pull the server forward so that the server rails expand and the retaining clips on the rails click into place.

7 Unplug and label the cable from the Ethernet port labeled LINK A on the dual NIC.

## Removing the cover of the Media Server

**CAUTION:**
Remove all power from the media server before starting this procedure.

1 Loosen the two captive screws on the back of the media server (see Figure 97, Locating the server cover's captive screws, on page 322.

2 Slide the server cover back from the front panel until the cover's tabs are released from the top slot of the front panel.

3 Lift the cover straight up and move it away from the server as shown in Figure 97, Locating the server cover's captive screws, on page 322.

**Figure 97: Locating the server cover's captive screws**

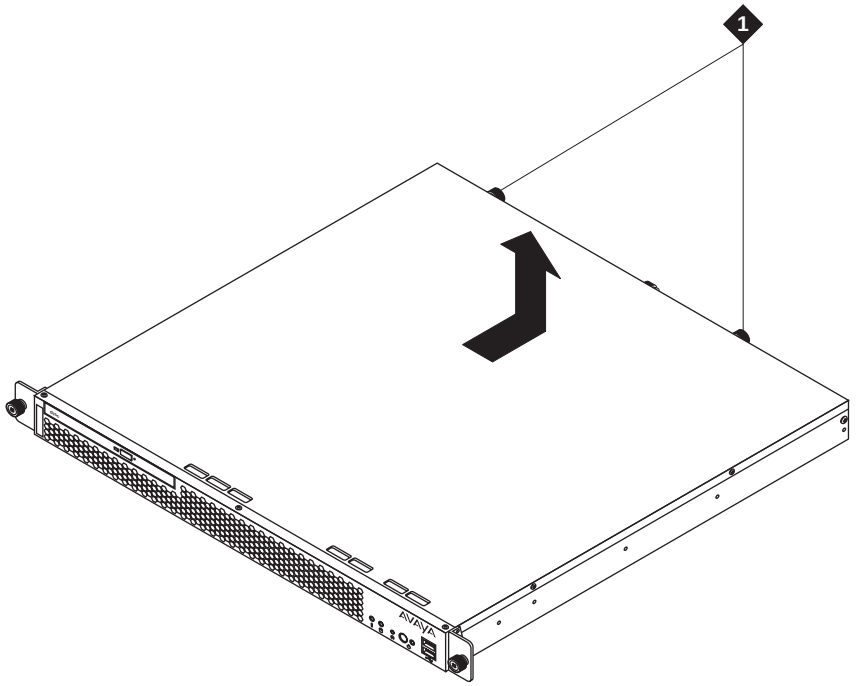



**Figure notes**

1 Server cover's captive screws

## Removing the fan unit

1. Locate the fan slot adjacent to the power plug on the rear of the server.
2. Remove the two screws holding the fan unit. You do not need to unplug the fan unit.
3. Set the adapter-support bracket to the right of the fan.

## Removing the old NIC

1. Completely unscrew the captive screw on the left hand side of the PCI-2 slot.

   The captive screw is now loose so that you can flip it up. You will need this space to maneuver the old NIC out of its slot.
2. Firmly pull the card out of its slot.

## Installing the small faceplate on the NIC

One type of NIC comes from the factory with a standard faceplate. You must remove this faceplate and replace it with a smaller one that fits the space. See Figure 98, Replacing the faceplate, on page 324.

If you have a NIC that does not require a small faceplate, proceed to Inserting the new NIC on page 324.

1. Using a #1 Phillips screwdriver, unscrew the two screws holding the larger faceplate.
2. Remove the faceplate from the NIC.
3. Position the small faceplate over the Ethernet ports. The faceplate must align with the screw holes on the circuit board.
4. Screw the small faceplate onto the circuit board using the two screws removed in step 1.

**Figure 98: Replacing the faceplate**

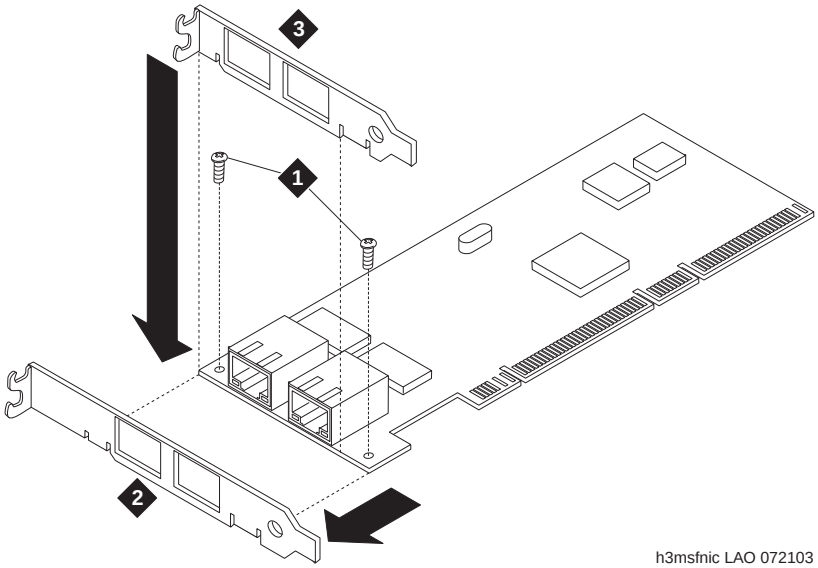



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Screws holding faceplate | **3** | Smaller faceplate |
| **2** | Faceplate on NIC shipped from factory | | |

## Inserting the new NIC

**1** Carefully grasp the new NIC by the top edge or upper corners and align it with the PCI-2 expansion slot. Press the NIC firmly into the expansion slot.

**WARNING:**

Ensure that the NIC is completely and correctly seated in the PCI-2 expansion slot of the S8500 Media Server. Incomplete insertion might cause damage to the system board or the NIC.

**2** Position the faceplate so that it fits in the PCI-2 slot using the captive screw to hold it in place.

**Figure 99: Repositioning the new NIC**

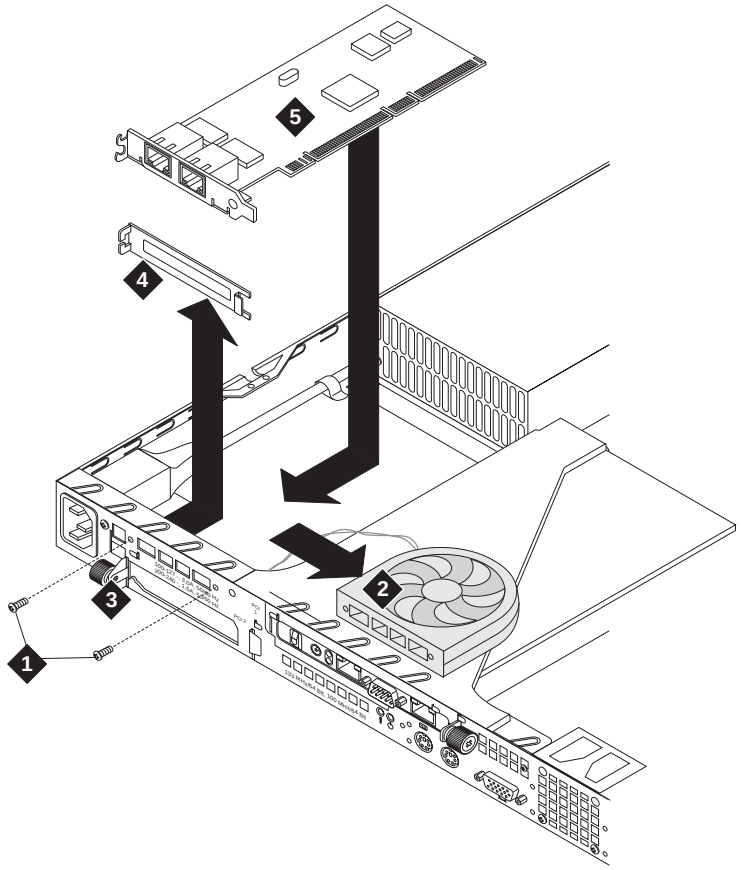



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Mounting screws | **4** | Smaller faceplate |
| **2** | Fan assembly | **5** | Network interface card |
| **3** | Captive screws | | |

## Replacing the fan unit

**1** Replace the fan unit with the fan blades pointed down toward the NIC., securing the fan unit with the two original screws.

## Replacing the cover and cabling

**1** Replace the cover onto the server.

**2** Slide the cover forward so the covers' tabs slide into place under the top slots of the front panel.

**3** Finger-tighten the thumb screws on the back of the server.

4 Release the retaining tabs on the rails and slide the S8500 Media Server back into place on the data rack.

5 Locate the marked cable that you removed from the old NIC and plug it into the Ethernet 2 port, which is labeled **ACT/LINK A** on the small faceplate of the new NIC.

## Powering up the server

Complete the following steps if you wish to start the media server at this time:

1 Plug the power cord into the power receptacle on back of the server.

2 Press the Power button located on the front right-hand side.

3 Login to the server after the startup to ensure that the installation is complete.

## Checking LED activity on the dual NIC

When the Media Server is back in service, check the LEDs on each port of the dual NIC (Figure 100, S8500 rear panel dual NIC LEDs, on page 326).

**Figure 100: S8500 rear panel dual NIC LEDs**

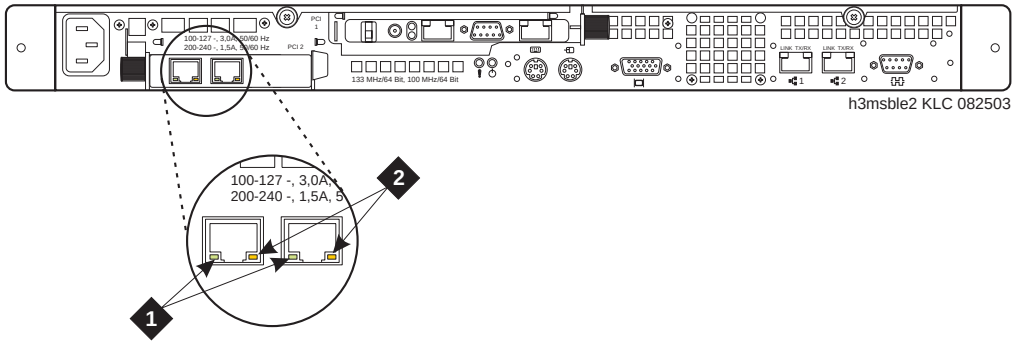



**Figure notes**

**1** Network activity LED (Tx/Rx)

**2** Connection rate:

- LED is off: there is a 10 BASE-T active link.
- LED is green: there is a 100 BASE-T active link.
- LED is orange: there is a 1000 BASE-T active link.

## Confirming original Ethernet configuration

After the Media Server is back in service, check the original Ethernet configuration settings:

1 Go to the **Configure Server** Web page.

2 Confirm that the server's Ethernet configuration settings are the same as before.

## Configuring the NIC

1. Under Server, click **Configure Server**
2. Click **Continue** through the review notices until you get to the ***xxx*** page.
3. Select **Configure Individual Services** and click **Continue**.
4. Select **Set Identities** and click **Continue**.
5. The following Ethernet ports are listed:
   - **Control Network A**: [default: Ethernet 0]
   - **Services Port**: [default: Ethernet 1]
   - **Corporate LAN**: [default: Ethernet 0]
   - **Unused**
6. Using the drop-down menu, set the **Corporate LAN** field to Ethernet 2 to have the IPSI control on a dedicated, separate Ethernet port.
7. Click **Continue**.
8. Fill in the following information for Ethernet 2:
   - IP address
   - Gateway
   - Subnet mask
   - Speed
9. Select “VLAN 802.1q priority tagging is enabled” if true.
10. Click **Change**. The status of the configuration update appears in the window.

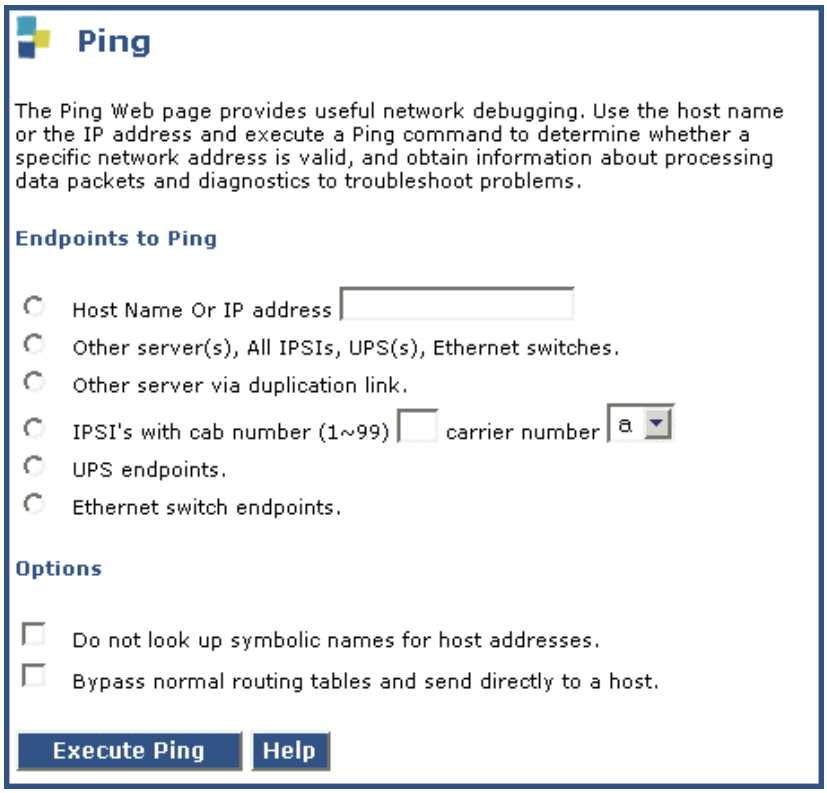
    When the update completes, the following message appears: `Successfully configured ethernet interfaces`.

## Testing connectivity to customer’s network

1. Under Diagnostics click **Ping**.

   The Ping screen displays (Figure 101, Ping screen, on page 328).

**Figure 101: Ping screen**




2 In the **Host Name or IP address** field, type in the host name or IP address of a computer on the network.

3 Click **Execute Ping**.

4 Verify that the ping was successful, indicating that the media server is connected to the customer's network.

5 If DNS is administered, type in the host name of a computer on the network.

6 Click **Execute Ping**.

7 Verify that the ping was successful, indicating that DNS is working.

If available, have a customer representative do the following test from a computer on their network:

1 Click **Start > Run** to open the ***Run*** dialog box.

2 Type **command** and click **OK** to open an MS-DOS command window.

3 Type **ping *serveripaddress*** and click **OK**, where ***serveripaddress*** is the IP address of media server.

4 Verify that the ping was successful.

5 If DNS is administered, type **ping *servername*** and press **Enter**, where ***servername*** is the host name of media server.

6 Verify that the ping was successful.

# S8700 component maintenance

This section contain information about:



## Replacing the S8700 Media Server

You might need to replace an Avaya S8700 Media Server to correct a problem, such as a functional failure of the motherboard, the hard drive, or other components. Depending on which software release that the failed media server is running, you might need to upgrade the software on the replacement media server and, perhaps, the existing media server.

### Upgrade requirements

A software upgrade might be required when replacing an S8700 Media Server. Table 74, Upgrade checklist, on page 329 describes when an upgrade is required.

**Table 74: Upgrade checklist**

| Software release before Media Server failure | Upgrade requirement |
|---|---|
| Release 1.0, 1.1.x (R011x.01.xxx.x) | If used, upgrade all LSPs to Release 1.2 software. Because the replacement media server comes with Release 1.2 software, you need to upgrade the existing media server to Release 1.2 software. |
| Release 1.2.x (R011x.02.xxx.x) | No upgrade is required because the replacement media server contains R1.2 software. However, a software patch, if necessary, must be installed. |
| Release 1.3.x (R011x.03.xxx.x) | Because the replacement media server contains R1.2 software, the software must be upgraded to R1.3. You must also install the same patch(es) as that on the existing media server. Neither the existing media server nor the LSPs need to be upgraded because they already have Release 1.3 software. |

### Required equipment

Verify that you have the following equipment and tools on site:

- Replacement S8700 Media Server
- CD-ROM(s) with appropriate software load(s) — R1.2 (1.0/1.1 replacement or for R1.0/1.1 LSPs) and/or R1.3 (R1.3 replacement)
- Ethernet crossover cable for direct connection of your laptop to the media servers
- Cross-point (Phillips) screwdrivers (#1 and #2)

- Hex-head (Allen) wrench (1/8 in.)
- Electrostatic wrist ground strap and mat.

## Pre-site tasks

In addition to the tasks listed in Table 75, Pre-site tasks for replacing an S8700 Media Server, on page 330, verify that the following tasks have been done:

- Ask the customer for the Product ID for the media server being replaced. If the customer does not have it, run the Avaya Registration Tool (ART) to obtain the Product ID number for replacement media server.
- If the customer is using SNMP for alarming, you need to get the IP addresses and community names from the customer as the SNMP programming is not saved after the replacement.
- If upgrading the software, verify that you have the correct software, software patches, and firmware. You must upgrade the firmware on the IPSIs, upgrade the software on both media servers, and install the required software patch.
- Verify that the customer has backed up all the system and translation files.

**Table 75: Pre-site tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | **(For R1.0, R1.1, and R1.3 replacements only)** Obtain CD-ROMs with the Correct Software Releases | Retrieve an R1.2 CD-ROM (1.0/1.1.x replacement or for R1.0/1.1 LSPs) and/or R1.3 CD-ROM (R1.3 replacement only).<br>**Note:** R1.2 systems do not require the CD-ROM because the replacement media server already has the R1.2 software. |
| | 2 | Get Communication Manager Patch, If Appropriate | The latest Communication Manager patch file may be available on the CD-ROM. Otherwise, download it to your laptop from the Avaya Support Web site (http//www.avaya.com/support). Select **Software & Firmware Downloads** > **S8700 Media Server** > **Software Download**. |
| | 3 | Get Firmware for IPSI, C-LAN, MedPro, and/or VAL Circuit Pack, If Appropriate | Download the latest firmware to your laptop from the Avaya Support Web site (http//www.avaya.com/support). Select **Software & Firmware Downloads > S8700 Media Server** > **Firmware Download**. |
| | 4 | Get the Product ID and Modem IP Address | Run ART to obtain the Product ID for the media server with the bad hard drive and the IP address for the customer's INADS line. Access the ART web site on your laptop at the URL, http://tscxp1.sd.avaya.com:8000/cgibin/ART/ARTstart.cgi. |
| | 5 | **(For R1.0/R1.1 replacement only)** Get License and Authentication Files | Go to the RFA Web site (http://rfa.avaya.com) to retrieve the License and Avaya Authentication files for the customer. You can use the files that were originally created. |

## Initial on-site tasks

**NOTE:**
Except where noted in the following checklist, see "Upgrading the Avaya S8700 Media Server Configurations" section on the *Avaya S8300 and Avaya S8700 Media Server Library* CD-ROM (555-233-825) for details on tasks.

**Table 76: Initial tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | Log into the Web Interface of the Active S8700 Media Server | Connect to the Services port on the back of the media server. Open a browser on your laptop, and using **192.11.13.6,** log onto the Maintenance Web Interface.<br>**Note:** You must use the initial installation craft password. |
| | 2 | Determine the Software Release of the Existing Media Server and Necessary Patches | **(For R1.2 and R1.3 replacement only)** Under Server Configuration and Upgrades, click **View Software Version**.<br>**(For R1.0/R1.1.x replacement only)** The system must be upgraded to R1.2 software. |
| | 3 | **(For R1.0/R1.1 replacement only)** Determine If the Customer Has LSPs | Ask the customer, or check by using a terminal emulator to access the Communication Manager SAT command prompt screen. Use the **192.11.13.6** IP address.<br>Type **list configuration media-gateway *number,*** where ***number*** is the number of a G700 media gateway. If **ICC** appears in slot 1, the device is an LSP. Repeat for each G700 Media Gateway. |
| | 4 | **(For R1.0/R1.1 replacement only)** If There Are LSPs, Upgrade LSPs and Their Respective G700 Media Gateways to R1.2 | The LSPs must be on R1.2 before upgrading the other media server to R1.2. Also, upgrade the firmware for each G700 Media Gateway, including media modules and P330 stack processors.<br>**Note:** Be sure to stop Communication Manager software on each LSP (use **stop -acfn** command) until the media server has been upgraded. For detailed information, see *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server, 555-234-100*. |
| | 5 | Determine If the Customer Has a Recent Backup of Data | On the Web Interface, select **View Backup Log** to search for backup files. Check for the types of data and dates. Verify that there are successful backups that could appropriately be restored, if necessary. Verify with the customer that if the backups were to a LAN server, you have access permissions to restore the data, if necessary. |

*(1 of 2)*

**Table 76: Initial tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 6 | Resolve Alarms on the Active Media Server | Under Alarms and Notification click **View Current Alarms**.<br>Use a terminal emulator to access the Communication Manager SAT command prompt screen. Use the **display alarms** command and resolve any alarms.<br>**Note**: You cannot resolve alarms on the standby media server. Also, DUP alarms on the active media server will re-occur. Ignore them for now. |
| | 7 | Back up All Data Sets from the Active S8700 Media Server | Under Data Backup/Restore select **Backup Now**.<br>**Note:** Be sure to check the **Save ACP translations prior to backup** option on the Backup Now page. |
| | 8 | Suppress Alarm Origination on the Active S8700 Media Server | Use telnet to access the Linux command line on the active media server. Use the **almsuppress -t 120** command to suppress alarms for the duration of the replacement process. (Maximum time is 2 hours.) |
| | 9 | Log into the Media Server Being Replaced, If Different<br>**Note**: Only if media server is functional. | Connect to the Services port on the back of the media server. Open a browser on your laptop, and using **192.11.13.6,** log onto the Maintenance Web Interface.<br>**Note:** You must use the initial installation craft password. |
| | 10 | Make Sure Media Server is in Standby Mode | Under Server click **View Summary Status**. Verify that the media server is in standby mode. |
| | 11 | Busy Out the Media Server | Under Server click **Busy Out Server**, then click **Busyout Server**. |
| | 12 | Shut Down the Media Server | Under Server, click **Shutdown This Server**.<br>Alternatively, use the shutdown button. See Shutting down the S8700 manually on page 341. |

*(2 of 2)*

## Replacing the S8700 Media Server

**Table 77: Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | Unplug the Media Server being replaced | Unplug the media server from its power source.<br>**Caution:** Turning off power in this way can corrupt data on the hard drive. Use this method to power down the media server only if you cannot shut it down. |
| | 2 | Disconnect All the Cables | Disconnect all the cables from the back of the failed media server.<br>**Note**: Be sure to label the cables for easy reconnection. |

*(1 of 2)*

**Table 77: Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 3 | Remove Media Server from Rack | Remove the media server from the rack. |
| | 4 | Replace the S8700 Media Server | See Remove the S8700 Media Server being replaced on page 338. |
| | 5 | Reinstall the Media Server in the Rack | Reinstall the media server in the rack. Leave all the cables unconnected. |
| | 6 | Power up the Replacement Media Server. | Plug the media server into the appropriate UPS to power it up. If it does not power up, press the power button on the front and release it quickly.<br>**Note:** Wait at least 3 minutes for the media server to complete its power up. Watch the LEDs on the media server to see when they stop flashing and stay solidly lit. |

*(2 of 2)*

## Final tasks

**Table 78: Final Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | Log onto the Replacement Media Server | Connect to the Services port on the back of the media server. Open a browser on your laptop, and using **192.11.13.6,** log onto the Maintenance Web Interface.<br>**Note**: You must use the initial installation craft password. |
| | 2 | Check That Processes are Running | Under Server click **View Process Status** and select **Summary and Display once**. Make sure all processes are up except dupmgr (the duplication cables are not connected yet). |
| | 3 | Set the Time and Date | Under Server click **Set Server Time/Timezone**. Make changes as necessary. |
| | 4 | Select Correct Configuration | Under Server Configuration and Upgrades click **Configure Server** and select IP Connect or Multi-Connect configuration, whichever is the appropriate configuration.<br>**Note**: The existing media server does not have this page because it disappears once the media server's offer type is configured. |

*(1 of 5)*

**Table 78: Final Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 5 | **(For R1.0/R1.1.x replacement only)** Download and Install the License And Authentication Files | Under Miscellaneous click **Upload Files to Server (via browser)** to upload the files from the laptop to the media server.<br>Click **Install License** and **Install Authentication** to install the files.<br>**Note**: The next time that you log in, you will be ASG challenged. |
| | 6 | **(For R1.3 replacement only)** Upgrade Software on the Media Server with the New Hard Drive to Match the Software Release on the Existing Media Server | Insert the software CD into the media server CD-ROM drive. Click **Install New Software Release** and continue through the software installation.<br>**Note**: Be sure to select **Make Server Upgrade Permanent** when the software upgrade is complete. |
| | 7 | Install Communication Manager Software Patch | Click **Upload Files to Server (via browser)** to copy the patch to the /var/home/ftp directory. Use telnet to access the Linux command prompt screen. Refer to *Avaya S8300 & S8700 Media Server Patching Procedures* available at http://avaya.com/support for the patch installation procedures.<br>**Note**: Installing the patch releases the media server into active service. |
| | 8 | Restore Configuration on the Replacement Media Server | Get the configuration data from the customer. Alternatively, log into the existing media server and under Server click **Configure Server** to view the configuration screens.<br>On the replacement media server, click **Configure Server** to restart the configure media server process. Use the configuration screens for the existing media server to determine the values for the new media server.<br>**Exception**: ensure that one Media Server is 1 and the other is 2.<br>**CAUTION:**<br>If you use the existing media server to retrieve the configure media server data, do **not** click Continue at the Update Server (Warning) screen. *You do not want to reconfigure the existing media server.* |
| | 9 | Restore Data on the Media Server with the New Hard Drive | Restore translations only. On the Maintenance Web Interface, click **View/Restore Data**.<br>**For 1.0/1.1.x only:** You must select **Force restore if backup version mismatch** also for the data to be restored to a different release of software. |

*(2 of 5)*

**Table 78: Final Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 10 | Verify the Software Version. | Under Server Configurations and Upgrades click **View Software Version** to verify that the replacement media server is on release 1.2 or 1.3 software, as appropriate, and has the appropriate patches. |
| | 11 | **(For 1.0/1.1.x Replacement Only)** Reset the System | At the SAT command prompt screen, use the **reset system 4** command. |
| | 12 | **(For 1.0/1.1.x Replacement Only)** Verify translations | At the SAT command prompt screen, use the **list station** command, and verify that the customer's stations are listed. |
| | 13 | **(For R1.0/R1.1.x replacement only)** Save Translations | On the SAT command prompt screen, use the **save translation** command. |
| | 14 | **(For R1.0/R1.1.x and R1.2 replacements only)** Upgrade IPSI, C-LAN, MedPro, and VAL Circuit Pack Firmware | The IPSI circuit packs must be on the latest firmware for an R1.2 system. At the same time, upgrade the firmware on the C-LAN, MedPro, and VAL circuit packs. Refer to "Upgrading the S8700 Media Server Configuration" section of the *Avaya S8300 and Avaya S8700 Media Server Library* CD-ROM (555-233-825).<br><br>**CAUTION:**<br>Upgrading the firmware on a circuit pack requires a reset of that circuit pack. |
| | 15 | Check the Configuration | On the SAT command prompt screen, use the **list configuration all** command. Check that all the hardware is displayed. |
| | 16 | Stop Communication Manager and Busy Out the Media Server | At the Linux command line, type **stop -acf**.<br><br>On the Maintenance Web Interface under Server, click Busy Out Server to busy out the Media Server. |
| | 17 | Restart Communication Manager on the Standby Media Server | At the Linux command line, type **start -ac** to bring the media server up in the busied out, standby mode. |
| | 18 | Verify Busied Out Status | Under Server click View Summary Status. Make sure the media server is busied out. |
| | 19 | Reattach All Cables | Connect the fiber duplication cable and the Ethernet duplication cable to the replacement media server. Connect all the other cables. |
| | 20 | Check the Status of the Standby Media Server from the Active Media Server | Connect to the active media server. Click **View Summary** Status. Make sure that the active media server shows data for the standby media server. |
| | 21 | Check the Status of the Active Media Server from the Standby Media Server | Connect to the standby media server. Click **View Summary** Status. Make sure that the standby media server shows data for the active media server and that the data from both media servers matches. |

*(3 of 5)*

**Table 78: Final Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 22 | Ping the Connections on the Replacement Media Server | Under Diagnostics click **Execute Pingall**. Ensure that all connections, including the active media server, the IPSI circuit packs, and all administered connections respond. |
| | 23 | Check Alarms on Both Media Server | Under Alarms and Notification click **View Current Alarms**. Clear any alarms that appear.<br>Connect to the active media server. On the SAT command prompt screen, use the **display alarms** command. Clear any alarms that appear.<br>Caution: If you cannot clear alarms, stop. Call your service support group. Do not continue with this task list until alarms have been resolved. |
| | 24 | Check the Health of the Active Media Server | On the SAT command prompt screen, use the **list ipserver-interface** and the **status health** commands. Check that all connections are working correctly. |
| | 25 | Release the Busied Out Standby Media Server | Connect to the standby media server. Under Server click **Release Server** to release the media server from busy out mode. The active media server will begin to refresh the translations and security files of the standby media server. |
| | 26 | Monitor the Refresh of the Standby Media Server | Connect to the active media server. Under Server click **View Summary Status** to monitor the refresh of the standby media server until the refresh is complete. |
| | 27 | Save Translations on the Active Media Server | Once the media server is refreshed, on the SAT command prompt screen, use the **save translation** command. |
| | 28 | Log in Again to the Standby Media Server Web Interface | Connect to the standby media server. Open a browser on your laptop, and using **192.11.13.6,** log into the Maintenance Web Interface. You should be ASG challenged in order to log in.<br>**Note**: You should no longer be able to use the initial installation craft password.<br>**(For R1.2 and R1.3 replacements only)** Go to Set the Product ID on the Replacement Media Server **on page 337**. |
| | 29 | **(For R1.0/R1.1.x replacement only)** Make the Standby Media Server the Active Media Server | Under Server click **Interchange Servers.** Also, select **Force interchange regardless of server status**.<br>This forces a reset system 4. Monitor the media server to make sure it is healthy before continuing. |
| | 30 | **(For R1.0/R1.1.x replacement only)** Check the Status of the Active Media Server | On the SAT command prompt screen, use the **list trunks**, **list stations**, **list hunt**, and **list data** commands to make sure that the same items that were in service before the replacement are still in service. |

*(4 of 5)*

**Table 78: Final Tasks for replacing an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 31 | **(For R1.0/R1.1.x replacement only)** Resolve Alarms on Both Media Servers | On the active media server first, click **View Current Alarms**. Then resolve alarms. Resolve alarms on the standby media server.<br>On the SAT command prompt screen, use the **display alarms** command. |
| | 32 | **(For R1.0/R1.1.x replacement only)** Log on to the Existing Media Server | Connect to the services port on the back of the media server that was not replaced, and using **192.11.13.6**, log onto the Maintenance Web Interface. |
| | 33 | **(For R1.0/R1.1.x replacement only)** Upgrade the Existing Media Server | Insert the R1.2 software CD into the existing media server CD-ROM drive. Under Server Configuration and Upgrades click **Install New Software Release** and continue through the software installation.<br>**Note**: Be sure to select **Make Server Upgrade Permanent** before continuing. |
| | 34 | **(For R1.0/R1.1 replacement only)** Install Software Patch on Existing Media Server | Under Miscellaneous click **Upload Files to Server** to copy the patch to the /var/home/ftp directory. Refer to *Avaya S8300 & S8700 Media Server Patching Procedures* available at http://avaya.com/support. |
| | 35 | **(For R1.0/R1.1 replacement only)** Release the Existing Media Server from Busy Out Mode | Under Server click **Release Server** to verify that the media server is released from the busy out mode. |
| | 36 | **(For R1.0/R1.1.x replacement only)** Start Call Processing on LSPs, If Present | Connect to each LSP, telnet to the IP address for that LSP and use the **start -afcn** command to restart call processing. |
| | 37 | Set the Product ID on the Replacement Media Server | Type **productid *-p product_id***, where product_id is the product ID you received from the customer or the ART tool. It should be the same product ID as the old media server. |
| | 38 | Enable Alarms to INADS on the Replacement Media Server | Using telnet on the Linux command prompt screen, type **almcall** to find out phone numbers, **almenable -d** to enable dial-out alarms, **almenable -s** to enable SNMP alarm traps, and **almenable** to verify that the alarms are enabled. |
| | 39 | Administer Backup Schedule on the Replacement Media Server | On the Maintenance Web interface under Data Backup/Restore, click **Schedule Backup** to readminister the media server's backup schedule. |
| | 40 | Backup System Files on Active Media Server | Click **Backup Now** and select "Save ACP translations prior to backup" to save translations and backup system files to the PCMCIA flashcard or to the customer's LAN backup media server. |
| | 41 | Log Off All Administration Applications | When you have completed all the administration, log off the media server. |

***(5 of 5)***

## Remove the S8700 Media Server being replaced

1. Using a cross-point screwdriver, unscrew one screw from each side.
2. Unscrew the remaining screws.
3. Carefully remove the media server from the rack.

## Install the replacement S8700 Media Server

**NOTE:**
If reusing the hard drive from the failed media server, go to Reusing the hard drive on page 338 before installing the replacement media server in the rack.

Refer to *Getting Started with the Avaya S8700 Media Server with the Avaya G650 Media Gateway, 555-245-703* for information on installing the S8700 Media Server in the rack and reconnecting all the cables.

## Reusing the hard drive

If the hard drive in the failed media server is still good, then you may want to reuse it in the replacement media server. Use the following processes to switch the hard drives:

- Remove the cover of the failed S8700 Media Server
- Remove the hard drive
- Replace the cover on the failed S8700 Media Server
- Remove the cover of the replacement S8700 Media Server
- Remove the hard drive
- Install the old hard drive
- Replace the cover of the replacement S8700 Media Server
- Return equipment

**CAUTION:**
Wear an anti-static wrist ground strap whenever handling components such as the hard drive of an Avaya S8700 Media Server. Connect the strap to an approved ground, such as an unpainted metal surface. Also, place the hard drive on an anti-static mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

### *Remove the cover of the failed S8700 Media Server*

1. Set the media server down on a flat surface with an electrostatic mat.
2. With your hex-head wrench, remove the 4 screws (see Media Server cover removal and replacement on page 339) that hold the brackets on to the side of the media server. Removing these screws also allows you to release the media server cover on the sides.
3. Use a #2 cross-point (Phillips) screwdriver to unscrew the two screws at the back of the media server that hold the cover in place (see Media Server cover removal and replacement on page 339).

4 Slide the media server cover back from the front panel (see Figure 102, Media Server cover removal and replacement, on page 339) until the cover's tabs are released from the top slot of front panel.

5 Lift the cover straight up and remove it from the media server.

**Figure 102: Media Server cover removal and replacement**

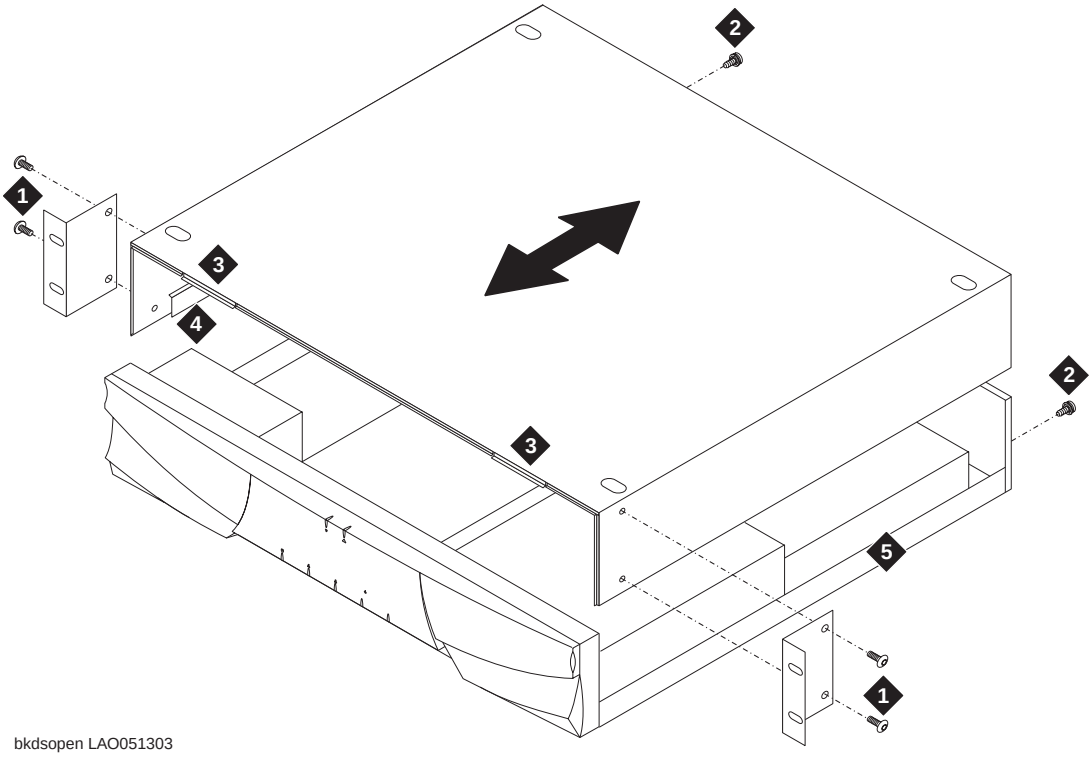



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Hex-head bracket screws | **4** | Inner rail guide |
| **2** | Cross-point (Phillips) cover screws | **5** | Bottom rail of media server |
| **3** | S8700 media server cover tabs | | |

### *Remove the hard drive*

1 Open the bezel on the front of the media server, if necessary, and use a #2 cross-point (Phillips) screwdriver to unscrew the two screws on the faceplate of the hard drive bracket.

**NOTE:**
The hard drive bracket is on the front right-hand side of the S8700 Media Server.

2 Partially pull out the hard drive bracket (Figure 103, Hard drive bracket and hard drive, on page 340) so that you can disconnect the cables. Note the position of the ribbon cable within the chassis so you can return it to exactly the same position later.

3 Unplug the 4-wire power cable from the back of the hard drive (Figure 103, Hard drive bracket and hard drive, on page 340).

4 Unplug the ribbon cable from the back of the hard drive (Figure 103, Hard drive bracket and hard drive, on page 340). Note that the red stripe on the ribbon cable is on the side closest to the power cable.

5 Pull the hard drive bracket from the media server, and place the hard drive and bracket assembly on your antistatic mat.

**NOTE:**
There is no need to remove the hard drive from the bracket.

**Figure 103: Hard drive bracket and hard drive**

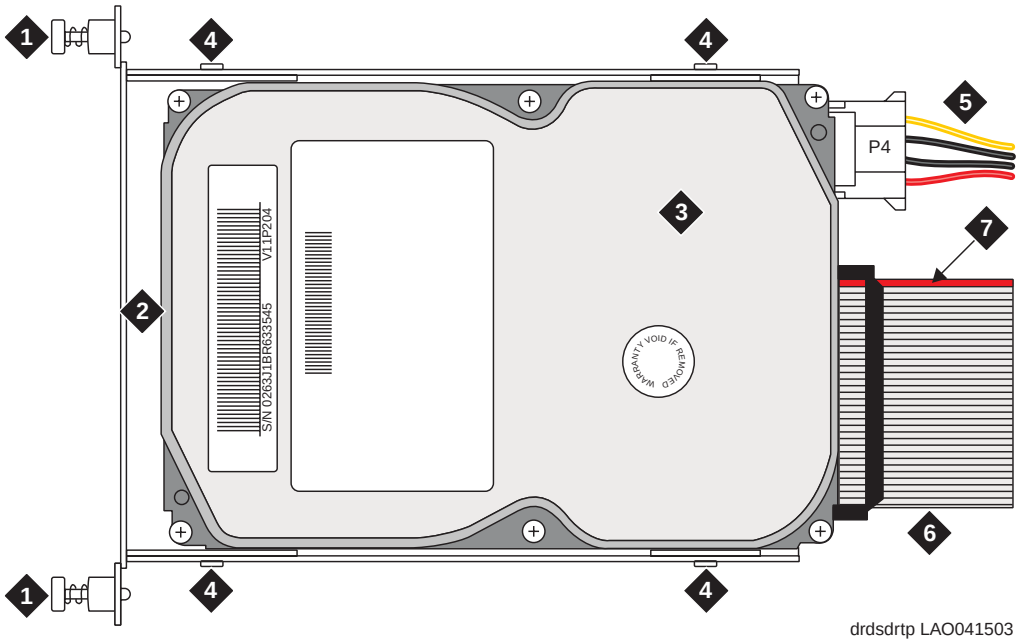



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Faceplate screw | **5** | Power cable |
| **2** | 1/8 to 1/4 inch gap | **6** | Ribbon cable |
| **3** | Hard drive | **7** | Position of red stripe |
| **4** | Bracket screws | | |

### *Replace the cover on the failed S8700 Media Server*

1 Replace the cover onto the media server (Figure 102, Media Server cover removal and replacement, on page 339). Be sure the guides on the inner sides of the cover set correctly on the bottom rails of the media server.

2 Slide the media server cover forward so that the covers' tabs slide into place under the top slots of the front panel.

3 Screw the two cross-point (Phillips) screws into the back of the media server to hold the cover in place (Figure 102, Media Server cover removal and replacement, on page 339).

4 Reattach the brackets to the side with the hex-head screws.

### *Remove the cover of the replacement S8700 Media Server*

1 Follow the steps in Remove the cover of the failed S8700 Media Server on page 338.

### *Remove the hard drive*

1 Follow the steps in Remove the hard drive on page 339.

### *Install the old hard drive*

1 Attach the ribbon cable to the back of the bracket. Be sure the red stripe on the cable is on the side closest to the power cable.

2 Attach the power cable (Figure 103, Hard drive bracket and hard drive, on page 340).

3 Lay the ribbon cable into the media server housing as it was before disconnecting it. This prevents bunching of the cable when you slide the hard drive bracket back into the media server.

4 Slide the hard drive bracket into the media server (Figure 103, Hard drive bracket and hard drive, on page 340), and hand-tighten the screws on the faceplate to secure it to the media server. Do *not* tighten the screws with a screwdriver.

**CAUTION:**
Be sure the ribbon cable is pushed completely inside the media server and is not bunched, pinched, or caught between the top of the hard drive and the hard drive slot.

### *Replace the cover of the replacement S8700 Media Server*

1 Follow the steps in Replace the cover on the failed S8700 Media Server on page 340.

2 Return to Tasks for replacing an S8700 Media Server on page 332 to continue with the listed tasks.

### *Return equipment*

1 Return both the failed media server and good hard drive.

## Shutting down the S8700 manually

This section contains procedures for shutting down the media server manually.

If you cannot access the Maintenance Web Interface, you may shut down the standby media server by following manual steps with the shutdown button:

1 Open the door on the front of the standby S8700 Media Server.

2 Press the media server shutdown button and release it quickly.

**CAUTION:**
Do not hold down the power button for more than a split second. Holding the button down too long causes a reboot of the media server. If you press the button properly, the LEDs do not change, and there is no response to indicate any changes to the system.

3 Press the media server shutdown button again and hold it down until the LEDs go out.

The LEDs on the media server flash and then go dark. The media server is shut down. Though the middle network LED (number 1) may not go out, the media server is still shut down and ready for replacement.

**CAUTION:**
Do not release the power button until all the LEDs go dark. If you release the button too early, the media server does not shut down.

# Replacing the S8700 hard drive

## Upgrade requirements

A software upgrade may be required when replacing a failed hard drive on an S8700 Media Server. The following table describes when an upgrade is required.

| Software release before disk failure | Upgrade requirement |
|---|---|
| Release 1.0, 1.1.x (R011x.01.xxx.x) | If used, upgrade all LSPs to Release 1.2 software. Because the replacement hard drive comes with Release 1.2 software, you need to upgrade the existing media server to Release 1.2 software. |
| Release 1.2.x (R011x.02.xxx.x) | No upgrade is required because the new hard drive contains R1.2 software. However, a software patch, if necessary, must be installed. |
| Release 1.3.x (R011x.03.xxx.x) | Because the new hard drive contains R1.2 software, the software must be upgraded to R1.3. You must also install the same patch(es) as that on the existing server. Neither the other media server nor the LSPs need to be upgraded because they already have R1.3 software. |

## Required equipment

Verify that you have the following equipment and tools on site:

- Replacement hard drive
- CD-ROM(s) with appropriate software load(s) — R1.2 (1.0/1.1 replacement or for R1.0/1.1 LSPs) and/or R1.3 (R1.3 replacement)
- Ethernet crossover cable for direct connection of your laptop to the media servers
- Cross-point (Phillips) screwdrivers (#1 and #2)
- Hex-head (Allen) wrench (1/8 in. 3mm)
- Electrostatic wrist ground strap and mat

## Pre-site tasks

Before you go on site, verify that the following tasks have been done.

- Ask the customer for the Product ID for the media server being replaced. If the customer does not have it, run the Avaya Registration Tool (ART) to obtain the Product ID number for the replacement media server.
- If the customer is using SNMP for alarming, you will need to get the IP addresses and community names from the customer as the SNMP programming is not saved after the replacement.

- If upgrading the software, verify that you have the correct software, software patches, and firmware. You must upgrade the firmware on the IPSIs, upgrade the software on both media servers, and install the required software patch.
- Verify that the customer has backed up all the system and translation files.

**Table 79: Pre-site tasks for replacing a hard drive on an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | **(For R1.0/1.1.x, R1.3 replacements only)** Obtain CD-ROMs with the Correct Software Releases | Retrieve an R1.2 CD-ROM (1.0/1.1.x replacement or for R1.0/1.1 LSPs) and/or R1.3 CD-ROM (R1.3 replacement only).<br>**Note:** R1.2 systems do not require the CD-ROM because the replacement hard drive already has the R1.2 software. |
| | 2 | Get Communication Manager Patch, If Appropriate | The latest Communication Manager patch file may be available on the CD-ROM. Otherwise, download it to your laptop from the Avaya Support Web site (http//www.avaya.com/support). Select **Software & Firmware Downloads > S8700 Media Server > Software Download**. |
| | 3 | Get Firmware for IPSI, C-LAN, MedPro, and/or VAL Circuit Pack, If Appropriate | Download the latest firmware to your laptop from the Avaya Support Centre Web site (http//www.avaya.com/support). Select **Software & Firmware Downloads > S8700 Media Server > Firmware Download**. |
| | 4 | Get the Product ID and Modem IP Address | Run ART to obtain the Product ID for the media server with the failed hard drive and the IP address for the customer's INADS line. Access the ART web site on your laptop at the URL http://art.dr.avaya.com/ARTidcrt.cgi. |
| | 5 | **(For R1.0/R1.1 replacement only)** Get License and Authentication Files | Go to the RFA Web site (http://rfa.avaya.com) to retrieve the License and Avaya Authentication files for the customer. You can use the files that were originally created. |

## Initial on-site tasks

**NOTE:**
Except where noted in Table 80, Initial tasks for replacing a hard drive on an S8700 Media Server, on page 344, see "Upgrading the Avaya S8700 Media Server Configurations" documentation on the *Avaya S8300 and S8700 Media Server Library CD-ROM, 555-233-825*, for detailed task lists.

**Table 80: Initial tasks for replacing a hard drive on an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | Log into Web interface of the active S8700 Media Server | Connect to the Services port on the back of the media server. Open a browser on your laptop, and using **192.11.13.6,** log onto the Maintenance Web Interface.<br><br>**Note:** You must use the initial installation craft password. |
| | 2 | Determine the Software Release of the Existing Media Server and Necessary Patches | **(For R1.2 and R1.3 replacement only)** Under Server Configuration and Upgrades, click **View Software Version**.<br><br>**(For R1.0/R1.1.x replacement only)** The system must be upgraded to R1.2 software. |
| | 3 | **(For R1.0/R1.1 replacement only)** Determine If the Customer Has LSPs | Ask the customer, or check by using a terminal emulator to access the Communication Manager SAT command prompt screen. Use the **192.11.13.6** IP address.<br>Type **list configuration media-gateway *number,*** where ***number*** is the number of a G700 media gateway. If **ICC** appears in slot 1, the device is an LSP. Repeat for each G700 Media Gateway. |
| | 4 | **(For R1.0/R1.1 replacement only)** If There Are LSPs, Upgrade LSPs and Their Respective G700 Media Gateways to R1.2 | The LSPs must be on R1.2 before upgrading the other media server to R1.2. Also, upgrade the firmware for each G700 Media Gateway, including media modules and P330 stack processors.<br><br>**Note:** Be sure to stop Communication Manager software on each LSP (use **stop -acfn** command) until the media server has been upgraded. For detailed information, see *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server, 555-234-100*. |
| | 6 | Determine If the Customer Has a Recent Backup of Data | On the Web Interface, select **View Backup Log** to search for backup files. Check for the types of data and dates. Verify that there are successful backups that could appropriately be restored, if necessary. Verify with the customer that if the backups were to a LAN server, you have access permissions to restore the data, if necessary. |
| | 7 | Resolve Alarms on the Active Media Server | Under Alarms and Notification click **View Current Alarms**.<br><br>Use a terminal emulator to access the Communication Manager SAT command prompt screen. Use the **display alarms** command.<br><br>For instructions on resolving alarms, see *Maintenance Alarms Reference (555-245-102)*<br><br>**Note:** You cannot resolve alarms on the standby media server. Also, DUP alarms on the active media server will re-occur. Ignore them for now. |
| | 8 | Back up All Data Sets from the Active S8700 Media Server | Under Data Backup/Restore select **Backup Now**.<br><br>**Note:** Be sure to check the **Save ACP translations prior to backup** option on the Backup Now page. |

***(1 of 2)***

**Table 80: Initial tasks for replacing a hard drive on an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 9 | Suppress Alarm Origination on the Active S8700 Media Server | Use telnet to access the Linux command line on the active media server. Use the **almsuppress -t 120** command to suppress alarms for the duration of the replacement process. (Maximum time is 2 hours.) |

*(2 of 2)*

## Tasks to replace the hard drive

**Table 81: Tasks for replacing the hard drive on an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | Unplug the Media Server with the Failed Hard Drive | Unplug the media server from its power source.<br>**CAUTION:**<br>Turning off power in this way can corrupt data on the hard drive. Use this method to power down the media server only when you are ready to replace the failed hard drive. |
| | 2 | Disconnect All the Cables | Disconnect all the cables from the back of the media server with the failed hard drive.<br>**Note:** Be sure to label the cables for easy reconnection. |
| | 3 | Remove Media Server from Rack | Remove the media server from the rack. |
| | 4 | Remove the Cover of the S8700 Media Server | See Remove the cover of the failed S8700 Media Server on page 338. |
| | 5 | Replace the Hard Drive | See Remove the S8700 Media Server being replaced on page 338. |
| | 6 | Replace the Cover of the S8700 Media Server | See Replace the cover of the replacement S8700 Media Server on page 341. |
| | 7 | Reinstall the Media Server in the Rack | Reinstall the media server in the rack. Leave all the cables unconnected. |
| | 8 | Power up the Media Server with the Replaced Hard Drive. | Plug the media server into the appropriate UPS to power it up. If it does not power up, press the power button and release it quickly.<br>**Note:** Wait at least 3 minutes for the media server to complete its power up. Watch the LEDs on the media server to see when they stop flashing and stay solidly lit. |

## Final tasks

**Table 82: Final tasks for replacing a hard drive in an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 1 | Log into the Maintenance Web Interface on the Media Server with the New Hard Drive | Connect to the Services port on the back of the media server. Open a browser on your laptop, and using **192.11.13.6,** log onto the Maintenance Web Interface.<br>**Note:** You must use the initial installation craft password. |
| | 2 | Check That Processes Are Running | Under Server click **View Process Status** and select "Summary and Display once." Make sure all processes are up except dupmgr (the duplication cables are not connected yet). |
| | 3 | Set the Time and Date | Under Server click **Set Server Time/Timezone**. Make changes as necessary. |
| | 4 | Select Correct Configuration | Under Server Configuration and Upgrades click **Configure Server** and select IP Connect or Multi-Connect configuration, whichever is the appropriate configuration.<br>**Note:** The existing media server does not have this page because it disappears once the media server's offer type is configured. |
| | 5 | **(For R1.0/R1.1.x replacement only)** Download and Install the License and Authentication Files | Under Miscellaneous click **Upload Files to Server (via browser)** to upload the files from the laptop to the media server.<br>Click **Install License** and **Install Authentication** to install the files.<br>**Note**: The next time you log in, you will be ASG challenged. |
| | 6 | **(For R1.3 replacement only)** Upgrade Software on the Media Server with the New Hard Drive to Match the Software Release on the Existing Media Server | Insert the software CD into the media server CD-ROM drive. Click **Install New Software Release** and continue through the software installation.<br>**Note:** Be sure to select **Make Server Upgrade Permanent** when the software upgrade is complete. |
| | 7 | Install Communication Manager Software Patch | Click **Upload Files to Server (via browser)** to copy the patch to the /var/home/ftp directory. Use telnet to access the Linux command prompt screen. Refer to *Avaya S8300 & S8700 Media Server Patching Procedures* available at http://avaya.com/support for the patch installation procedures.<br>**Note**: Installing the patch releases the media server into active service. |

*(1 of 5)*

**Table 82: Final tasks for replacing a hard drive in an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 8 | Restore Configuration on the Media Server with the New Hard Drive | Get the configuration data from the customer. Alternatively, log into the existing media server and under Server Configuration and Upgrades click **Configure Server** to view the configuration screens.<br><br>On the media server with the new hard drive, click **Configure Server** to restart the configure media server process. Use the configuration screens for the existing media server to determine the values for the media server you are configuring. **Exception**: make sure that one media server is 1 and the other is 2.<br><br>**Caution:** If you use the existing media server to retrieve the configure media server data, do **not** click Continue at the Update Server (Warning) screen. *You do not want to reconfigure the existing media server*. |
| | 9 | Restore Data on the Media Server with the New Hard Drive | Restore translations only. Under Data Backup/Restore click **View/Restore Data**.<br><br>**For 1.0/1.1.x only:** You must select **Force restore if backup version mismatch** also for the data to be restored to a different release of software. |
| | 10 | Verify the Software Version. | Under Server Configurations and Upgrades click **View Software Version** to verify that the media server with the new hard drive is on release 1.2 or 1.3 software, as appropriate, and has the appropriate patches. |
| | 11 | **(For 1.0/1.1.x Replacement Only)** Reset the System | At the SAT command prompt screen, use the **reset system 4** command. |
| | 12 | **(For 1.0/1.1.x Replacement Only)** Verify translations | At the SAT command prompt screen, use the **list station** command, and verify that the customer's stations are listed. |
| | 13 | **(For R1.0/R1.1.x replacement only)** Save Translations | At the SAT command prompt screen, use the **save translation** command. |
| | 14 | **(For R1.0/R1.1.x and R1.2 replacements only)** Upgrade IPSI, C-LAN, MedPro, and VAL Circuit Pack Firmware | The IPSI circuit packs must be on the latest firmware for an R1.2 system. At the same time, upgrade the firmware on the C-LAN, MedPro, and VAL circuit packs. Refer to "Upgrading the S8700 Media Server Configuration" section of the *Avaya S8300 and Avaya S8700 Media Server Library* CD-ROM (555-233-825).<br><br>**CAUTION:**<br>Upgrading the firmware on a circuit pack requires a reset of that circuit pack. |
| | 15 | Check the Configuration | At the SAT command prompt screen, use the **list configuration all** command. Check that all the hardware is displayed. |

*(2 of 5)*

**Table 82: Final tasks for replacing a hard drive in an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 16 | Stop Communication Manager and Busy Out the Media Server | At the Linux command line, type **stop -acf**.<br>On the Maintenance Web Interface, under Server click **Busy Out Server** to busy out the media server. |
| | 17 | Restart Communication Manager on the Media Server | At the Linux command line, type **start -ac** to bring the media server up in the busied out, standby mode. |
| | 18 | Verify Busied Out Status | On the Maintenance Web Interface under Server click **View Summary Status**. Make sure the media server is busied out. |
| | 19 | Reattach All Cables | Connect the fiber duplication cable and the Ethernet duplication cable to the media server with the new hard drive. Connect all the other cables. |
| | 20 | Check the Status of the Standby Media Server from the Active Media Server | Connect to the active media server. Click **View Summary Status**. Make sure that the active media server shows data for the standby media server. |
| | 21 | Check the Status of the Active Media Server from the Standby Media Server | Connect to the standby media server. Click **View Summary Status**. Make sure that the standby media server shows data for the active media server and that the data from both media servers matches. |
| | 22 | Ping the Connections on the Media Server with the New Hard Drive | Under Diagnostics click **Execute Pingall**. Ensure that all connections, including the active media server, the IPSI boards, and all administered connections respond. |
| | 23 | Check Alarms on Both Media Server | Under Alarms and Notification click **View Current Alarms**. Clear any alarms that appear.<br>Connect to the active media server. On the SAT command prompt screen, use the **display alarms** command. Clear any alarms that appear.<br>**Caution**: *If you cannot clear alarms, stop.* Call your service support group. Do not continue with this task list until alarms have been resolved. |
| | 24 | Check the Health of the Active Media Server | At the SAT command prompt screen, use the **list ipserver-interface** and the **status health** commands. Check that all connections are working correctly. |
| | 25 | Release the Busied Out Standby Media Server | Connect to the standby media server. Under Server click **Release Server** to release the media server from busy out mode. The active media server will begin to refresh the translations and security files of the standby media server. |
| | 26 | Monitor the Refresh of the Standby Media Server | Connect to the active media server. Under Server click **View Summary Status** to monitor the refresh of the standby media server until the refresh is complete. |

*(3 of 5)*

**Table 82: Final tasks for replacing a hard drive in an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 27 | Save Translations on the Active Media Server | Once the media server is refreshed, on the SAT command prompt screen, use the **save translation** command. |
| | 28 | Log in Again to the Standby Media Server Web Interface | Connect to the standby media server. Open a browser on your laptop, and using **192.11.13.6,** log into the Maintenance Web Interface. You should be ASG challenged in order to log in.<br>**Note:** You should no longer be able to use the initial installation craft password.<br>**(For R1.2 and R1.3 replacements only)** Go to Set the Product ID on the Replacement Media Server **on page 337**. |
| | 29 | **(For R1.0/R1.1.x replacement only)** Make the Standby Media Server the Active Media Server | Under Server click **Interchange Servers.** Also, select **Force interchange regardless of server status** to make the standby media server the active media server.<br>**Note**: This forces a reset system 4. Monitor the media server to make sure it is healthy before continuing. |
| | 30 | **(For R1.0/R1.1.x replacement only)** Check the Status of the Active Media Server | At the SAT command prompt screen, use the **list trunks**, **list stations**, **list hunt**, and **list data** commands to make sure that the same items that were in service before the replacement are still in service. |
| | 31 | **(For R1.0/R1.1.x replacement only)** Resolve Alarms on Both Media Servers | On the active media server first, click **View Current Alarms**. Then resolve alarms. Connect to the standby media server and resolve alarms on the standby media server.<br>On the SAT command prompt screen, use the **display alarms** command. |
| | 32 | **(For R1.0/R1.1.x replacement only)** Log into the Existing Media Server | Connect to the Services port on the back of the media server that did *not* need a hard drive replacement and using **192.11.13.6,** log into the Maintenance Web Interface |
| | 33 | **(For R1.0/R1.1.x replacement only)** Upgrade the Existing Media Server | Insert the R1.2 software CD into the existing media server CD-ROM drive. Under Server Configuration and Upgrade click **Install New Software Release** and continue through the software installation.<br>**Note:** Be sure to select **Make Server Upgrade Permanent** before continuing. |
| | 34 | **(For R1.0/R1.1.x replacement only)** Install Software Patch on Existing Media Server | Under Miscellaneous click **Upload Files to Server (via browser)** to copy the patch to the /var/home/ftp directory. Refer to *Avaya S8300 & S8700 Media Server Patching Procedures* available at http://avaya.com/support. |

*(4 of 5)*

**Table 82: Final tasks for replacing a hard drive in an S8700 Media Server**

| ✓ | | Task | Description |
|---|---|---|---|
| | 35 | **(For R1.0/R1.1.x replacement only)** Release the Existing Media Server from Busy Out Mode | Under Server click **Release Server** to verify that the media server is released from the busy out mode. |
| | 36 | **(For R1.0/R1.1.x replacement only)** Start Call Processing on LSPs, If Present | Connect to each LSP, telnet to the IP address for that LSP and use the **start -afcn** command to restart call processing. |
| | 37 | Set the Product ID on the Media Server with the New Hard Drive | Type **productid -p *product_id, where product_id*** is the product ID you received from the customer or the ART tool. It should be the same product ID as the old hard drive. |
| | 38 | Enable Alarms to INADS on the Media Server with the New Hard Drive | Using telnet on the Linux command prompt screen, type **almcall** to find out phone numbers, **almenable -d** to enable dial-out alarms, **almenable -s** to enable SNMP alarm traps, and **almenable** to verify that the alarms are enabled. |
| | 39 | Administer Backup Schedule on the Media Server with the New Hard Drive | On the Maintenance Web interface under Data Backup/Restore, click **Schedule Backup** to readminister the media server's backup schedule. |
| | 40 | Backup System Files on Active Media Server | Click **Backup Now** and select "Save ACP translations prior to backup" to save translations and backup system files to the PCMCIA flashcard or to the customer's LAN backup media server. |
| | 41 | Log Off All Administration Applications | When you have completed all the administration, log off of the media server. |

*(5 of 5)*

## Replace the hard drive

**CAUTION:**
Wear an antistatic wrist ground strap whenever handling components such as the hard drive of an Avaya S8700 Media Server. Connect the strap to an approved ground, such as an unpainted metal surface. Also, place the hard drive on an antistatic mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

### *Remove the cover of the S8700 Media Server*

1. Set the media server down on a flat surface with an electrostatic mat.
2. With your hex-head wrench, remove the 4 screws (Figure 104, Media Server cover removal and replacement, on page 351) that hold the brackets on to the side of the media server. Removing these screws also allows you to release the media server cover on the sides.

3 Use a #1 cross-point (Phillips) screwdriver to unscrew the two screws at the back of the media server that hold the cover in place (Figure 104, Media Server cover removal and replacement, on page 351).

4 Slide the media server cover back from the front panel (Figure 104, Media Server cover removal and replacement, on page 351) until the cover's tabs are released from the top slot of the front panel.

5 Lift the cover straight up and remove it from the media server.

**Figure 104: Media Server cover removal and replacement**

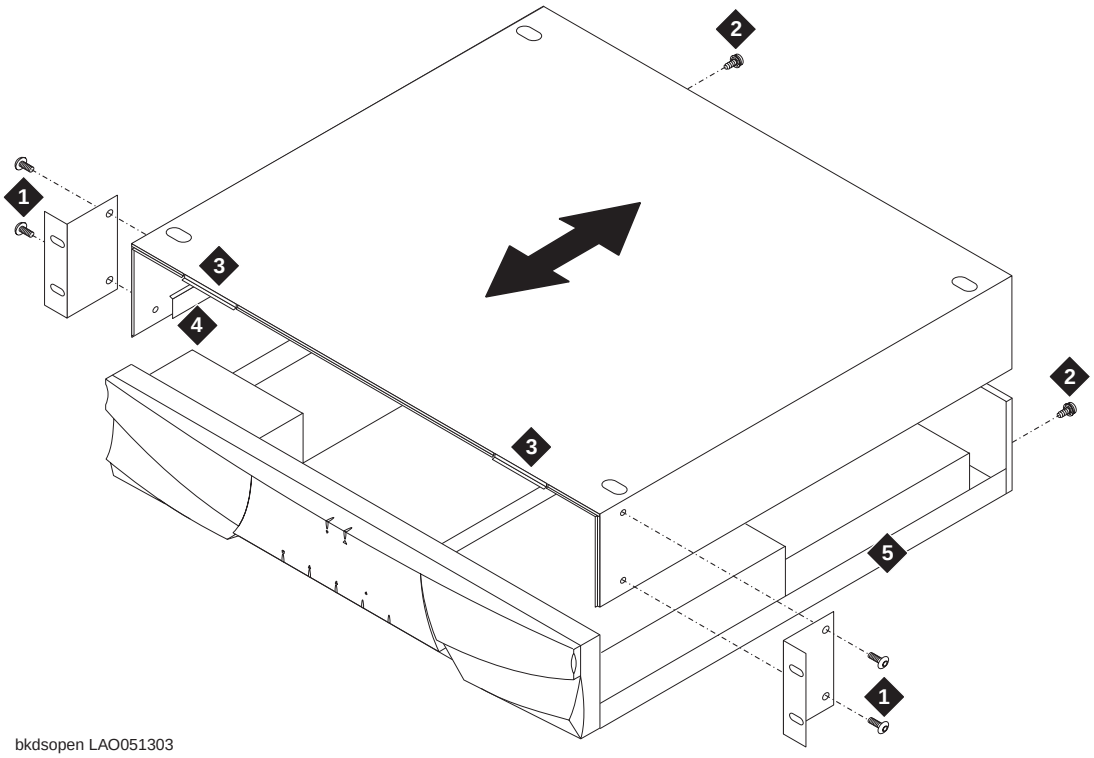



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Hex-head bracket screws | **4** | Inner rail guide |
| **2** | Cross-point (Phillips) cover screws | **5** | Bottom rail of media server |
| **3** | S8700 media server cover tabs | | |

### *Remove the hard drive*

1 Open the bezel on the front of the media server, if necessary, and use a #2 cross-point (Phillips) screwdriver to unscrew the two screws on the faceplate of the hard drive bracket.

**NOTE:**
The hard drive bracket is on the front right-hand side of the S8700 Media Server.

2 Partially pull out the hard drive bracket (Figure 105, Hard drive bracket and hard drive, on page 352) so that you can disconnect the cables. Note the position of the ribbon cable within the chassis so you can return it to exactly the same position later.

3 Unplug the 4-wire power cable from the back of the hard drive (Figure 105, Hard drive bracket and hard drive, on page 352).

4 Unplug the ribbon cable from the back of the hard drive (Figure 105, Hard drive bracket and hard drive, on page 352). Note that the red stripe on the ribbon cable is on the side closest to the power cable.

5 Pull the hard drive bracket from the media server, and place the hard drive and bracket assembly on your antistatic mat.

6 Unscrew the four screws holding the hard drive in the hard-drive bracket (Figure 105, Hard drive bracket and hard drive, on page 352). Remove the hard drive from the bracket.

**Figure 105: Hard drive bracket and hard drive**

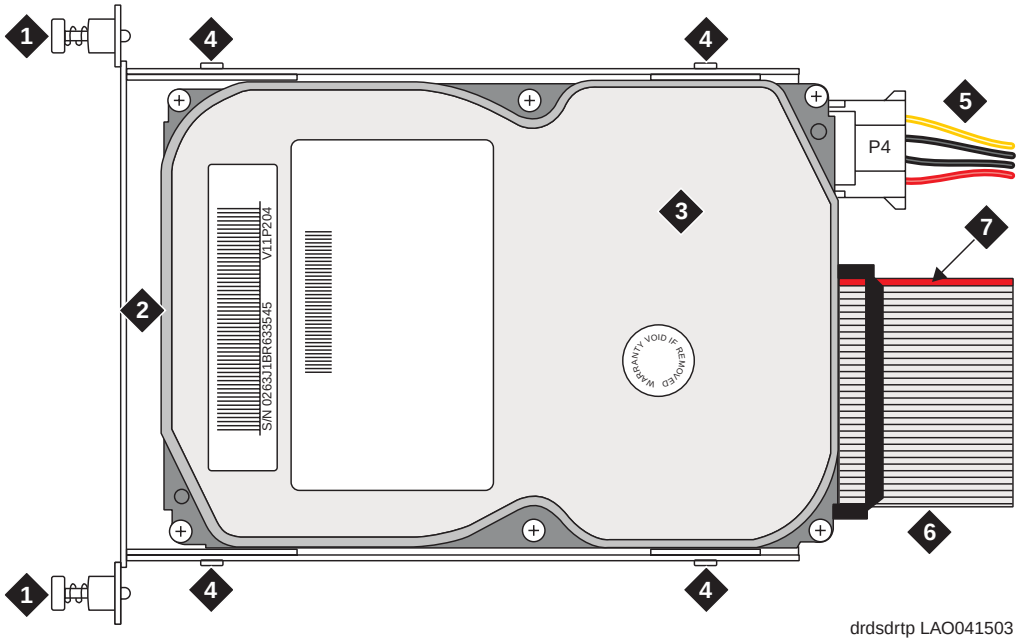



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Faceplate screw | **5** | Power cable |
| **2** | 1/8 to 1/4 inch gap | **6** | Ribbon cable |
| **3** | Hard drive | **7** | Position of red stripe |
| **4** | Bracket screws | | |

### *Install new hard drive*

1 Insert the new hard drive into the hard drive bracket so that the end of the hard drive is 1/8 to 1/4 inches from the faceplate of the bracket (Figure 105, Hard drive bracket and hard drive, on page 352).

2 Reinsert the four bracket screws to attach the hard drive to the bracket (Figure 105, Hard drive bracket and hard drive, on page 352).

3 Reattach the ribbon cable. Be sure the red stripe on the cable is on the side closest to the power cable.

4 Reattach the power cable (Figure 105, Hard drive bracket and hard drive, on page 352).

5 Lay the ribbon cable into the media server housing as it was before disconnecting it. This prevents bunching of the cable when you slide the hard drive bracket back into the media server.

6 Slide the hard drive bracket into the media server, and hand-tighten the screws on the faceplate to secure it to the media server. Do *not* tighten the screws with a screwdriver.

**CAUTION:**
Be sure the ribbon cable is pushed completely inside the media server and is not bunched, pinched, or caught between the top of the hard drive and the hard drive slot.

### *Replace the cover of the S8700 Media Server*

1 Replace the cover onto the media server (Figure 104, Media Server cover removal and replacement, on page 351). Be sure the inner rail guides of the cover set correctly on the bottom rails of the media server.

2 Slide the media server cover forward so the covers' tabs slide into place under the top slots of the front panel.

3 Screw the two cross-point (Phillips) screws into the back of the media server to hold the cover in place (Figure 104, Media Server cover removal and replacement, on page 351).

4 Reattach the brackets to the sides of the cover with the hex-head bracket screws.

5 Return to Table 81, Tasks for replacing the hard drive on an S8700 Media Server, on page 345 to continue with the listed tasks.

# G600 component maintenance

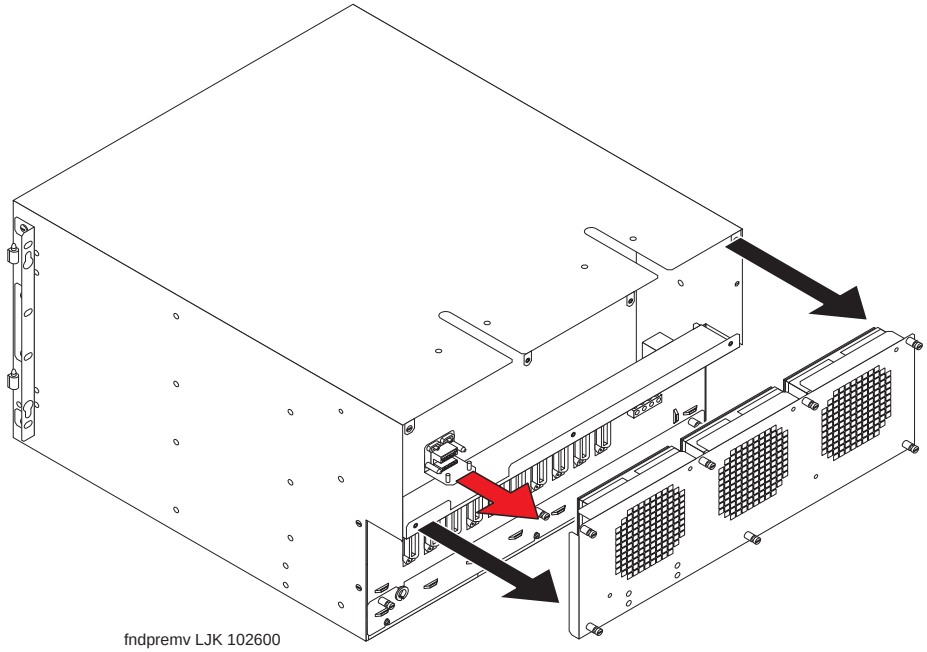
## G600 fan removal/replacement

**WARNING:**
You can remove the fan assembly while the system is running, but you must replace the new assembly within 60 seconds to avoid a thermal overload.

1 Place the new fan assembly close to the G600.

2 Loosen the thumb screws on the fan assembly, and pull it straight out (unplug it) as shown in Figure 106, Removing the G600 fan assembly, on page 354. The power for the fan automatically disconnects when the assembly is unplugged.

**Figure 106: Removing the G600 fan assembly**




3 Plug in the new fan assembly. The power for the fan automatically connects when the fan assembly is plugged in.

4 Tighten every thumb screw on the fan assembly.

# Replacing a BIU or rectifier

To remove a battery interface unit (BIU) or rectifier, first attach a grounding strap from the cabinet to your bare wrist, and then perform the following steps:

1 Unlock the latch pin.

2 Pull down on the locking lever until the BIU or rectifier moves forward and disconnects from its socket.

3 Pull the BIU or rectifier out just enough to break contact with the backplane connector. Use steady, even force to avoid disturbing the backplane.

4 Carefully slide the BIU or rectifier out of slot.

To install a BIU or rectifier, first attach a grounding strap from the cabinet to your bare wrist, and then perform the following steps:

1 Insert the back edge of the BIU or rectifier, making sure that it is horizontally aligned. Slide the unit into the slot until it engages the backplane. Use extreme care in seating the backplane connectors.

2 Lift the locking lever until the latch pin engages.

3 Verify that the unit is seated correctly by observing the operation of the LEDs.

# 9 Additional maintenance procedures

This chapter describes updates, tests and preventive measures not covered elsewhere in this book. It includes the following topics:



## Upgrading firmware

To update firmware on Avaya equipment use the information sources listed in Table 83, Firmware upgrade information sources, on page 355.

**Table 83: Firmware upgrade information sources**

| To upgrade firmware on | Use this information |
|---|---|
| TN circuit packs | FW-DWNLD (Firmware Download) in *Maintenance Alarms Reference (555-245-102)* |
| S8500 Media Server | *Upgrading Software and Firmware--Avaya S8500 Media Server* |
| S8700 Media Server | *Upgrading Software and Firmware--Avaya S8700 Media Server* |
| G700 Media Gateway | *Job Aid: Firmware Download Procedure for the G700 Media Gateway (555-245-758)* |

## DS1 CPE loopback jack (T1 only)

Using the DS1 CPE loopback jack, a technician can test the DS1 span between the system and the network interface point. The loopback jack is required when DC power appears at the interface to the Integrated Channel Service Unit (ICSU). The loopback jack isolates the ICSU from the DC power and properly loops the DC span power.

**NOTE:**
The loopback jack operates with any vintage of TN767E (or later) or TN464F (or later) DS1 circuit packs. The loopback jack operates with the 120A2 (or later) ICSU only; *not* the 31xx series of Channel Service Units (CSUs), other external CSUs, or earlier ICSUs.

# Loopback Jack installation

## Configurations using a Smart Jack

The preferred location of the loopback jack is at the interface to the smart jack. This provides maximum coverage of CPE wiring when remote tests are run using the loopback jack. If the smart jack is not accessible, install the loopback jack at the extended demarcation point.

1. If there is no extended demarcation point, install the loopback jack directly at the network interface point as shown in Figure 107, Network Interface at Smart Jack, on page 361.
2. If there is an extended demarcation point and the smart jack is not accessible, install the loopback jack as shown in Figure 108, Network Interface at Extended Demarcation Point (Smart Jack inaccessible), on page 362.
3. If there is an extended demarcation point, but the smart jack is accessible, install the loopback jack as shown in Figure 109, Network Interface at Extended Demarcation Point (Smart Jack accessible), on page 363.

## Configurations without a Smart Jack

Install the loopback jack at the point where the cabling from the ICSU plugs into the “dumb” block. If there is more than one “dumb” block, choose the one that is closest to the interface termination feed or the fiber MUX. This provides maximum coverage for loopback jack tests. See Figure 110, Network Interface at “Dumb” Block, on page 364 and Figure 111, Network Interface at “Dumb” Block with repeater line to Fiber MUX, on page 365.

## Installation

To install the loopback jack:

1. Disconnect the RJ-48 (8-wide) connector (typically an H600-383 cable) at the appropriate interface point and connect the loopback jack in series with the DS1 span. See Figure 107, Network Interface at Smart Jack, on page 361 through Figure 111, Network Interface at “Dumb” Block with repeater line to Fiber MUX, on page 365.
2. Plug the H600-383 cable from the ICSU into the female connector on the loopback jack.
3. Plug the male connector on the loopback jack cable into the network interface point.

**NOTE:**
Do not remove the loopback jack after installation. This is not a test tool and should always be available to remotely test a DS1 span.

## Administration

1. At the management terminal, enter **change ds1** ***location*** (the DS1 Interface circuit pack for which the loopback jack was installed).
2. Be sure the `near-end CSU type` is set to **integrated**.
3. On page 2 of the screen, change the `supply CPE loopback jack power` field to **y**.

   **NOTE:**
   Setting this field to **y** informs the technician that a loopback jack is present on the facility. This allows a technician to determine that the facility is available for remote testing.

4. Enter **save translation** to save the new information.

## DS1 span test

This test should only be performed after the DS1 circuit pack and the 120A2 (or later) ICSU have been successfully tested using appropriate maintenance procedures. The DS1 span test consists of 2 sequential parts. Each part provides a result indicating if there is a problem in the CPE wiring. CPE wiring may be considered problem-free only if the results of both parts are successful.

The first part of the span test powers-up the loopback jack and attempts to send a simple code from the DS1 board, through the wiring and loopback jack, and back to the DS1 board. Maintenance software waits about 10 seconds for the loopback jack to loop, sends the indication of the test results to the management terminal, and proceeds to the second part of the test.

The second part of the test sends the standard DS1 3-in-24 stress testing pattern from the DS1 board, through the loopback jack, and back to a bit error detector and counter on the DS1 board. The bit error rate counter may be examined on the management terminal, and provides the results of the second part of the test. The test remains in this state until it is terminated so that the CPE wiring may be bit error rate tested for as long as desired.

1. Busy out the DS1 circuit pack by entering **busyout board** ***location***.
2. At the management terminal, enter **change ds1** ***location*** and verify the `near-end csu type` is set to **integrated**.
3. On page 2 of the DS1 administration screen, confirm that the `TX LBO` field is **0** (dB). If not, record the current value and change it to 0 dB for testing. Press **Enter** to implement the changes or press **Cancel** to change nothing.
4. Enter **test ds1-loop** ***location*** **cpe-loopback-jack**. This turns on simplex power to the loopback jack and waits about 20 seconds for any active DS1 facility alarms to clear. A “PASS” or “FAIL” displays on the terminal. This is the first of the two results. A “FAIL” indicates a fault is present in the wiring between the ICSU and the loopback jack. The loopback jack may also be faulty. A “PASS” only indicates that the loopback jack looped successfully, and not that the test data contains no errors. If a “PASS” is obtained, continue with the following steps.

   **NOTE:**
   The loss of signal (LOS) alarm (demand test #138) is not processed during this test while the 3-in-24 pattern is active.

5. Enter **clear meas ds1 loop** ***location*** to clear the bit error count.
6. Enter **clear meas ds1 log** ***location*** to clear the performance measurement counts.

7 Enter **clear meas ds1 esf *location*** to clear the ESF error count.

8 Enter **list meas ds1 sum *location*** to display the bit error count. Refer to Table 84, DS1 span troubleshooting, on page 358 for troubleshooting information.

**Table 84: DS1 span troubleshooting**

| Displayed Field | Function | Indication |
|---|---|---|
| Test: cpe-loopback-jack | Pattern 3-in-24 | The loopback jack test is active. |
| Synchronized | Y or N | • If **y** appears, the DS1 circuit pack has synchronized to the looped 3-in-24 pattern and is accumulating a count of the bit errors detected in the pattern until the test has ended.<br>• If **n** appears, retry the test five times by ending the test (Step 11) and re-starting the test (Step 4).<br>• If the circuit pack never synchronizes, substantial bit errors in the 3-in-24 pattern are likely. This could be intermittent connections or a broken wire in a receive or transmit pair in the CPE wiring. |
| Bit Error Count | Cumulative count of detected errors | If there are no wiring problems, the counter remains at 0.<br>A count that pegs at 65535 or continues to increment by several hundred to several thousand on each **list meas** command execution may indicate:<br>• Intermittent or corroded connections<br>• Severe crosstalk<br>• Impedance imbalances between the two conductors of the receive pair or the transmit pair. Wiring may need replacement.<br>Note that “ESF error events” counter and the ESF performance counter summaries (“errored seconds”, “bursty errored seconds”, and so forth) will also increment. These counters are not used with the loopback jack tests. However, they will increment if errors are occurring. Counters should be cleared following the test. |

9 Repeat Steps 5 through 8 as desired to observe bit error rate characteristics. Also, wait 1 to 10 minutes between Steps 5 through 7. One minute without errors translates to better than a 1 in 10 to the eighth error rate. Ten minutes without errors translates to better than a 1 in 10 to the ninth error rate.

**10** If the test runs for 1 minute with an error count of 0, confirm that the 3-in-24 pattern error detector is operating properly by entering **test ds1-loop *location* inject-single-bit-error**. This causes the 3-in-24 pattern generator on the DS1 circuit pack to inject a single-bit error into the transmit pattern. A subsequent **list meas ds1 summary *location*** command displays the bit error count:

- If a count greater than 1 is displayed, replace the ICSU and retest.
- If the problem continues, replace the DS1 circuit pack.

**11** Terminate the test by entering **test ds1-loop *location* end cpe-loopback-jack-test**. Wait about 30 seconds for the DS1 to re-frame on the incoming signal and clear DS1 facility alarms.

Loopback termination fails under the following conditions:

**a** The span is still looped somewhere. This could be at the loopback jack, at the ICSU, or somewhere in the network. This state is indicated by a fail code of 1313. If the red LED on the loopback jack is on, replace the ICSU. Re-run the test and verify that the loopback test terminates properly. If not, replace the DS1 circuit pack and repeat the test.

**b** The DS1 cannot frame on the incoming span's signal after the loopback jack is powered down. This means that there is something wrong with the receive signal into the loopback jack from the "dumb" block or the smart jack. If the service provider successfully looped and tested the span, up to the smart jack, this condition isolates the problem to the wiring between the loopback jack and the smart jack. Refer to Loopback Jack fault isolation procedures on page 359 for information about how to proceed in this case. The test cannot be successfully terminated until a good signal is received. To properly terminate the test before a good receive signal is available, enter **reset board *location***.

**12** Restore the "TX LBO" field to the original value recorded in Step 2.

**13** Release the DS1 circuit pack using the **release board *location*** command.

**14** Leave the loopback jack connected to the DS1 span.

# Loopback Jack fault isolation procedures

This section describes the possible DS1 configurations in which the loopback jack is used. These configurations are when:

- The DS1 provider includes a smart jack.
- No smart jack is provided at all.
- A site uses fiber multiplexers.

These configurations are separated into Configurations using a Smart Jack on page 359 and Configurations without a Smart Jack on page 363.

## Configurations using a Smart Jack

The addition of the loopback jack and the presence of a smart jack divides the DS1 span into three separate sections for fault isolation. These sections are described in Table 85, DS1 span section descriptions, on page 360.

**Table 85: DS1 span section descriptions**

| Section | Smart Jack location |
|---|---|
| Section 1: | Between the 120A2 (or later) ICSU and the loopback jack |
| Section 2: | Between the loopback jack and the smart jack (network interface point) |
| Section 3: | From the smart jack to the Central Office (CO). It is necessary to contact the DS1 provider to run this test. |

A problem can exist in one or more of the three sections. The field technician is responsible for finding and correcting problems in the first two sections. The DS1 service provider is responsible for finding and correcting problems in the third section. Testing is divided into three steps:

1. Test customer premises wiring (Span Section 1 in the following three figures) from the ICSU to the loopback jack as described in "DS1 Span Test."
2. Test the CO-to-network interface wiring (Section 3 in Figure 107, Network Interface at Smart Jack, on page 361) using the smart jack loopback (CO responsibility). Coordinate this test with the DS1 provider.
3. Test the short length of customer premises wiring (Span Section 2 in the following three figures) between the loopback jack and the smart jack. This can be done using a loopback that "overlaps" section 2 of the cable. Any of the following loopbacks can do this:
   a. The local ICSUs line loopback, which is typically activated, tested, and then deactivated by the DS1 service provider at the CO end.
   b. The local DS1 interface's payload loopback, activated and tested by the DS1 service provider at the CO end.
   c. The far-end ICSU's line loopback. This test is activated at the management terminal by entering **test ds1-loop *location* far-csu-loopback-test-begin**. The test is terminated by entering **test ds1-loop *location* end-loopback/span-test**. Bit error counts are examined as described in DS1 span test on page 357. This test method is the least preferable because it covers wiring that is not in the local portion of the span. This test only isolates problems to section 2 wiring if there are no problems in the wiring between the far-end CO and the far-end ICSU. Coordinate this test with the DS1 service provider.

   If any of the tests fails, a problem is indicated in Section 2 as long as the tests for Span Section 1 and Span Section 3 pass. Since Span Section 2 includes the network interface point, it is necessary to work with the service provider to isolate the fault to the loopback jack cable, the "dumb" block, or the smart jack.

**Figure 107: Network Interface at Smart Jack**

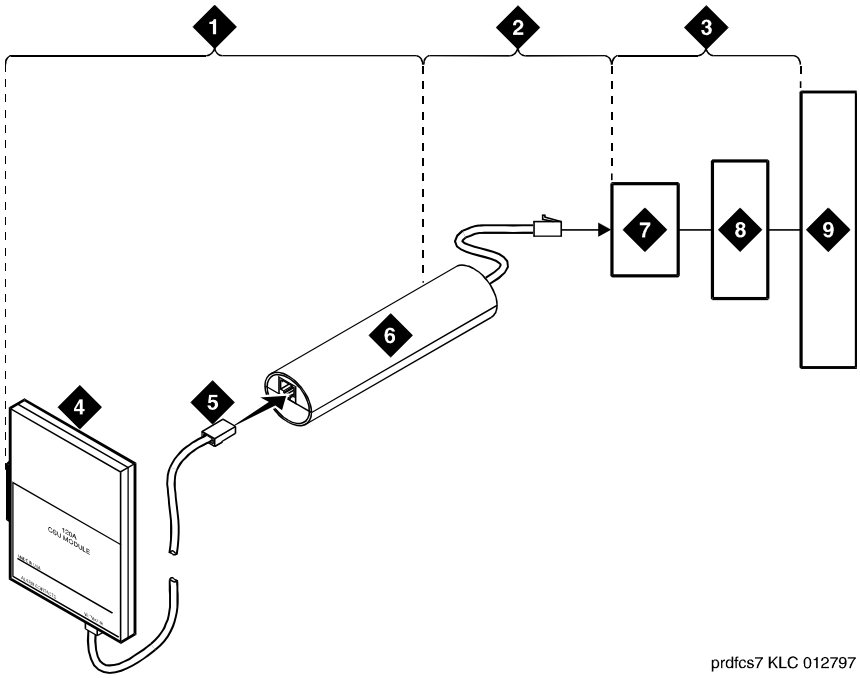



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Span Section 1 | **6** | Loopback Jack |
| **2** | Span Section 2 | **7** | Network Interface Smart Jack |
| **3** | Span Section 3 | **8** | Interface Termination or Fiber MUX |
| **4** | 120A2 (or later) Integrated Channel Service Unit (ICSU) | **9** | Central Office |
| **5** | RJ-48 to Network Interface (Up to 1000 Feet) (305 m) | | |

**Figure 108: Network Interface at Extended Demarcation Point (Smart Jack inaccessible)**

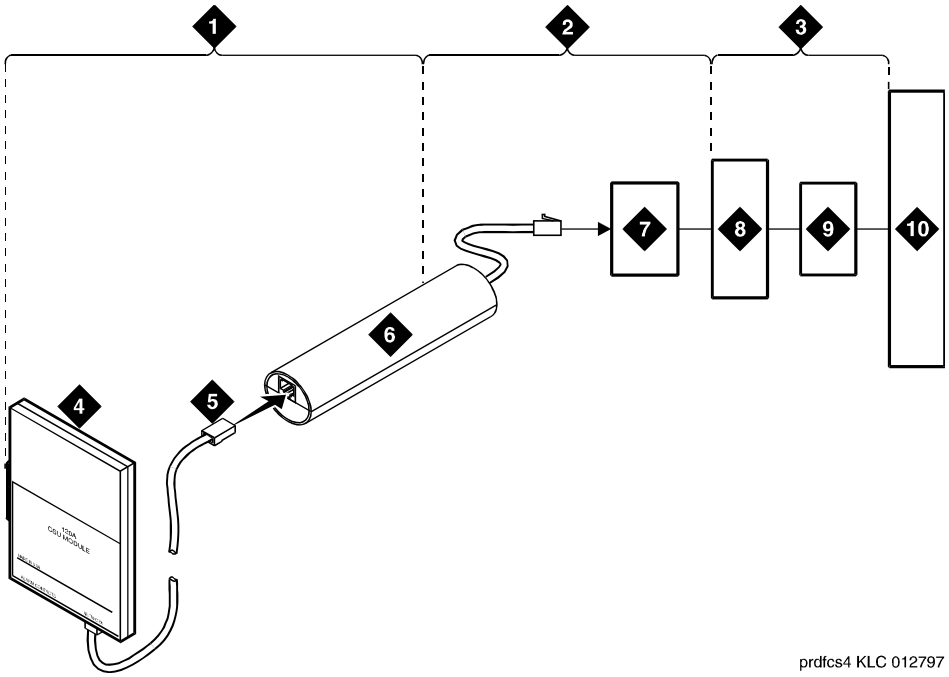



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Span Section 1 | **6** | Loopback Jack |
| **2** | Span Section 2 | **7** | “Dumb” Block (Extended Demarcation) |
| **3** | Span Section 3 | **8** | Network Interface Smart Jack |
| **4** | 120A2 (or later) Integrated Channel Service Unit (ICSU) | **9** | Interface Termination or Fiber MUX |
| **5** | RJ-48 to Network Interface (up to 1000 Feet) (305 m) | **10** | Central Office |

**Figure 109: Network Interface at Extended Demarcation Point (Smart Jack accessible)**

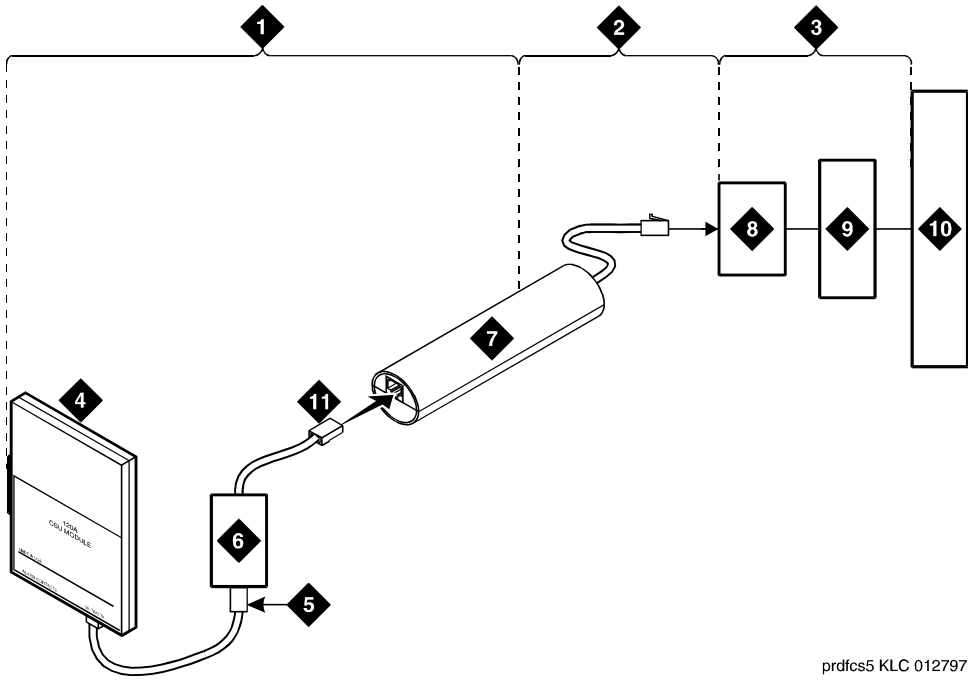



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Span Section 1 | **6** | "Dumb" Block (Extended Demarcation) |
| **2** | Span Section 2 | **7** | Loopback Jack |
| **3** | Span Section 3 | **8** | Network Interface Smart Jack |
| **4** | 120A2 (or later) Integrated Channel Service Unit (ICSU) | **9** | Interface Termination or Fiber MUX |
| **5** | RJ-48 to Network Interface (up to 1000 Feet) (305 m) | **10** | Central Office |
| | | **11** | "Dumb" Block to Smart Jack RJ-48 |

## Configurations without a Smart Jack

When the loopback jack is added to a span that does not contain a smart jack, the span is divided into two sections. See Figure 110, Network Interface at "Dumb" Block, on page 364 and Figure 111, Network Interface at "Dumb" Block with repeater line to Fiber MUX, on page 365. These sections are described in Table 86, DS1 span section descriptions (without a Smart Jack), on page 363.

**Table 86: DS1 span section descriptions (without a Smart Jack)**

| Span section | Smart Jack location |
|---|---|
| Span Section 1: | ICSU to the loopback jack |
| Span Section 2: | Loopback jack to the CO) |

**Figure 110: Network Interface at "Dumb" Block**

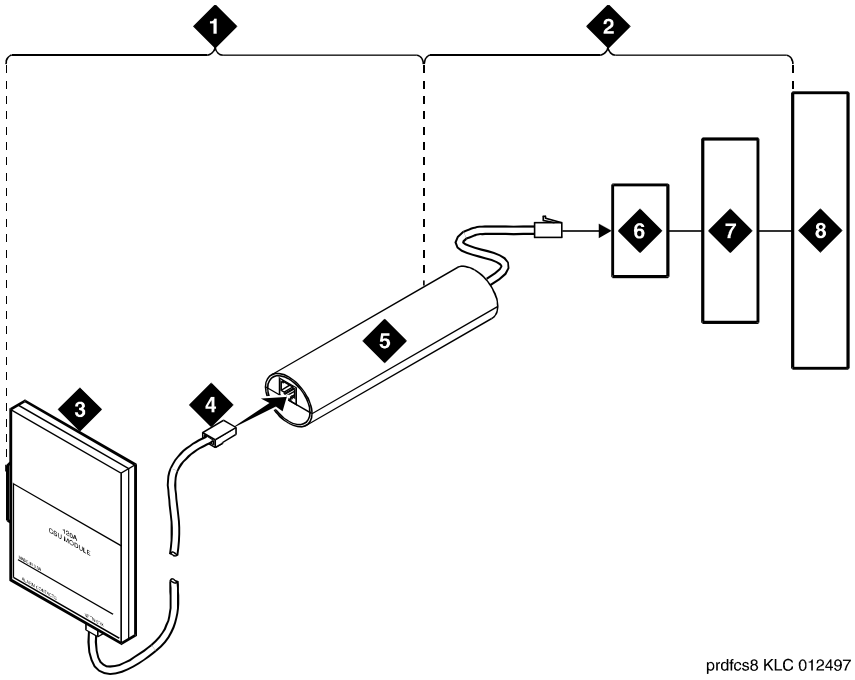



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Span Section 1 | **5** | Loopback Jack |
| **2** | Span Section 2 | **6** | "Dumb" Block (Demarcation Point) |
| **3** | 120A2 (or later) Integrated Channel Service Unit (ICSU) | **7** | Interface Termination or Fiber MUX |
| **4** | RJ-48 to Network Interface (up to 1000 Feet) (305 m) | **8** | Central Office |

**Figure 111: Network Interface at “Dumb” Block with repeater line to Fiber MUX**

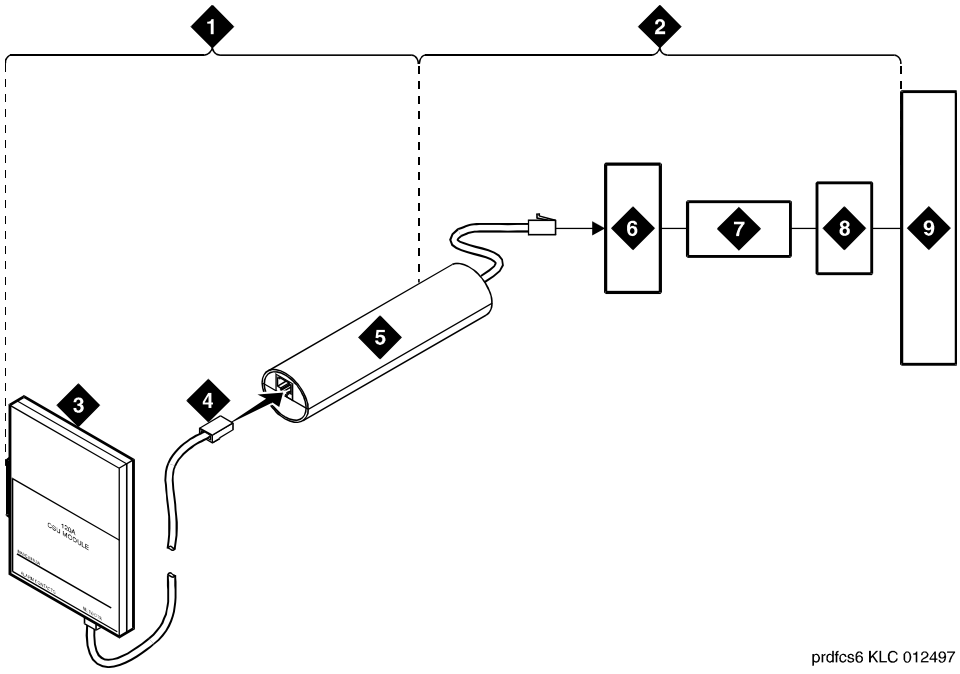



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Span Section 1 | **5** | Loopback Jack |
| **2** | Span Section 2 | **6** | “Dumb” Block (Demarcation Point) |
| **3** | 120A2 (or later) Integrated Channel Service Unit (ICSU) | **7** | Repeater |
| **4** | RJ-48 to Network Interface (up to 1000 Feet) (305 m) | **8** | Fiber MUX |
| | | **9** | Central Office |

Span Section 2 includes the short cable from the loopback jack to the “dumb” block demarcation point (part of the loopback jack). This is the only portion of section 2 that is part of customer premises wiring but is not covered in the loopback jack’s loopback path.

A problem can exist in one or both of the two sections. The field technician is responsible for finding and correcting problems in Span Section 1 and the loopback cable portion of Span Section 2. The DS1 service provider is responsible for finding and correcting problems in the majority of Span Section 2. Testing is divided into two steps:

1. Test customer premises wiring (section 1 in Figure 110, Network Interface at “Dumb” Block, on page 364) from the ICSU to the loopback jack as described in DS1 span test on page 357.
2. Test the loopback jack-to-”dumb” block and”dumb” block-to-CO wiring (Span Section 2 in Figure 110, Network Interface at “Dumb” Block, on page 364). This can be done using a loopback that “overlaps” the section of the span. Any of the following loopbacks can do this:
   a. The local ICSU’s line loopback, which is typically activated, tested, and then deactivated by the DS1 service provider at the CO end.

**b** The local DS1 interface's payload loopback, activated and tested by the DS1 service provider at the CO end.

**c** The far-end ICSU's line loopback. This test is activated at the management terminal by entering **test ds1-loop *location* far-csu-loopback-test-begin**. The test is terminated by entering **test ds1-loop *location* end-loopback/span-test**. Bit error counts are examined as described in the "DS1 Span Test" section. This test only isolates problems to Span Section 2 wiring if there are no problems in the wiring between the far-end CO and the far-end ICSU. Coordinate this test with the DS1 service provider.

If any of the above tests (a, b, or c) fail, a problem is indicated in Span Section 2. This could mean bad loopback jack -to-"dumb" block cabling, but is more likely to indicate a problem somewhere between the "dumb" block and the CO. This is the responsibility of the DS1 service provider. If the DS1 span test confirms that there are no problems in section 1, the technician should proceed as follows to avoid unnecessary dispatch.

- Identify and contact the DS1 service provider.
- Inform the DS1 provider that loopback tests of the CPE wiring to the "dumb" block (section 1) showed no problems.
- If the far-end ICSU line loopback test failed, inform the DS1 provider.
- Request that the DS1 provider perform a loopback test of their portion of the Span Section 2 wiring by sending someone out to loop Span Section 2 back to the CO at the "dumb" block.

  If this test fails, the problem is in the service provider's wiring.

  If the test passes, the problem is in the cable between the loopback jack and the "dumb" block. Replace the loopback jack.

## Configurations using fiber multiplexers

Use the loopback jack when customer premises DS1 wiring connects to an on-site fiber multiplexer (MUX) and allows wiring to the network interface point on the MUX to be remotely tested. This requires that ICSUs be used on DS1 wiring to the MUX.

Fiber MUXs can take the place of interface termination feeds as shown in

- Figure 107, Network Interface at Smart Jack, on page 361
- Figure 108, Network Interface at Extended Demarcation Point (Smart Jack inaccessible), on page 362
- Figure 109, Network Interface at Extended Demarcation Point (Smart Jack accessible), on page 363
- Figure 110, Network Interface at "Dumb" Block, on page 364.

Test these spans using the same procedures as metallic spans. Note the following points:

**1** Fiber MUXs may have loopback capabilities that can be activated by the service provider from the CO end. These may loop the signal back to the CO or back to the DS1 board. If the MUX provides the equivalent of a line loopback on the "problem" DS1 facility, this may be activated following a successful loopback jack test and used to isolate problems to the wiring between the loopback jack and the MUX.

2 Be aware that there are installations that use repeated metallic lines between the MUX and the "dumb" block. These lines require DC power for the repeaters and this DC power is present at the "dumb" block interface to the CPE equipment. *A loopback jack is required in this configuration to properly isolate and terminate the DC power.*

To check for the presence of DC, make the following four measurements at the network interface jack:

1 From Transmit Tip (T, Pin 5) to Receive Tip (T1, Pin 2)

2 From Transmit Ring (R, Pin 4) to Receive Ring (R1, Pin 4)

3 From Transmit Tip (T, Pin 5) to Transmit Ring (R, Pin 4)

4 From Receive Tip (T1, Pin 2) to Receive Ring (R1, Pin 4)

Every measurement should read 0 (zero) volts DC. For pin numbers and pin designations, refer to *DEFINITY Communications System Generic 1, Generic 2 and Generic 3 V1 and 2 - Integrated Channel Service Unit (CSU) Module Installation and Operation*, 555-230-193.

# Facility test calls

The facility test calls feature allows you to use a voice terminal to make test calls to specific trunks, time slots, tones, and tone receivers 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 screen, and you must know the facility test call access code. The code can be retrieved by entering **display feature-access-codes**. It appears on page one of the screen output.

**NOTE:**
For the ISDN-PRI test call feature see Troubleshooting ISDN-PRI test calls on page 215.

The following test call descriptions are for voice terminal users.

## Trunk 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. 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. **S8700**: 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. **S8100**: If the trunk is on an S8100 PN port, dial the 6-digit port number **PCSSpp**, where:
   - P = Port network number (1)
   - C = Carrier number (A=1, B=2, C=3)
   - SS = Slot number (01-10)
   - pp = Port number
   - The channels on a DS1 trunk are addressed by using the channel number for the port number.
4. **S8300** / **G700**: If the trunk is on a G700 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 - 4, 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,

   **a** Dial FAC.

   **b** Get dial tone.

   **c** Dial 0348305.

**5** Listen for one of the following call progress tones:

| If you get... | Then... |
|---|---|
| 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. |

**NOTE:**
For a definition of call progress tones, refer to *Overview for Avaya Communication Manager, 555-233-767*.

**6** 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.

## DS0 Loop-Around test call

The DS0 loop-around feature provides a loop-around connection for incoming non-ISDN DS1 trunk data calls. This feature is similar to the far-end loop-around connection provided for the ISDN test call feature. This DS0 loop around is provided primarily to allow a network service provider to perform facility testing at the DS0 level before video teleconferencing terminals are installed at the PBX.

The feature is activated on a call-by-call basis by dialing a test call extension specified on the second page of the System Parameters Maintenance screen. No special hardware is required. When the test call extension is received by the PBX, a non inverting 64-kbps connection is set up on the PBX's time division multiplexed bus. More than one loop-around call can be active at the same time.

For calls routed over the public network using the ACCUNET Switched Digital Service (SDS) or Software-Defined Data Network (SDDN), the data-transmission rate is 56 kbps since robbed bit signaling is used. For calls established over a private network using common-channel signaling, the full 64-kbps data rate is available.

On the Trunk Group screen:

- Set the communications type to **data** when the incoming trunk group is used only for data calls (SDS).
- Set the communications type to **rbavd** (robbed bit alternate voice data) when the incoming trunk group is used for robbed bit alternate voice and/or data (SDN/SDDN).
- Set the communications type to **avd** for private network trunks using common channel signaling.

## DTMR test call

This call accesses and tests the dual-tone multifrequency receivers (DTMR-PTs) located on TN718, TN420, TN744, TN748, TN756, and TN2182 tone detector circuit packs. These tone receivers are also known as touch-tone receivers (TTRs). Before making the test call, use **list configuration** to determine the location of the circuit packs that you want to test.

All eight ports of circuit packs TN744 and TN2182 are DTMR ports. All the other packs have just four DTMR ports: 01, 02, 05 and 06.

To place a tone receiver test call:

1. Dial the FAC described in the introduction to this section and listen for dial tone.
2. Dial the seven-digit port location ***UUCSSpp*** of one of the DTMR ports located on a Tone Detector circuit pack:

   C = Carrier number (A = 1, B = 2, C = 3, D = 4, E = 5)

   SS = Slot number (00 – 20)

   pp = Port circuit number
3. Listen for one of the following call progress tones:

| If you get... | Then... |
|---|---|
| Confirmation tone | The DTMR is connected. Go to Step 4. |
| Intercept tone | The port entered is not a TTR or the board is not inserted (if a trunk, see above). |
| Reorder tone | The DTMR is in use (call processing), the board is busied out, or inter-PN resources are unavailable for the call. |
| Dial tone | The port is a trunk. See the preceding section. |

**NOTE:**
For a definition of call progress tones, refer to *Overview for Avaya Communication Manager, 555-233-767*.

4. Dial the sequence **1234567890*#**.

   If the sequence is entered and received correctly, dial tone is returned and another test call can be made. If the test fails, intercept tone is returned. A failure may indicate a faulty DTMR port or circuit pack, a faulty voice terminal, or an error in the entry of the sequence.
5. To test another DTMR, repeat Steps 2 through 4.
6. To terminate the test call, hang up the station set used for testing.

## TDM bus time slot test call

The time slot test call connects the voice terminal to a specified time slot on the A or B TDM Bus of a specified port network. To connect to any out-of-service time slots, refer to Out-of-Service time slot test call on page 372.

To test a specific time slot on the TDM bus of a specific port network:

1. Dial the FAC described in the introduction to this section and listen for dial tone.
2. Dial the 2-digit port network number followed by # and the 3-digit time slot number listed in Table 87, TDM Bus time slot numbers, on page 371.
3. Listen for one of the following call progress tones:

| If you get... | Then... |
|---|---|
| Reorder tone | The time slot is in use, the time slot is not addressable, or inter-PN resources are not available to make the call. |
| Confirmation tone | The time slot is idle or out-of-service. The time slot may be on the TDM bus (A or B) that is not currently carrying tones, or it may be busied out. The call is connected to the time slot so that any noise may be heard. |
| System tone | The time slot is carrying a system tone as listed in Table 87, TDM Bus time slot numbers, on page 371. |

**NOTE:**
For a definition of call progress tones, refer to *Overview for Avaya Communication Manager, 555-233-767*.

## TDM bus time slots

When you address a tone-carrying time slot on the TDM bus (A or B) that is currently carrying tones, you will be connected to that time slot and will hear the tone as follows:

- Time slots 005 – 021 and 261 – 277 (bus A) are reserved to carry the system's dedicated tones.
- Time slots 000 – 004 and 256 – 260 (bus B) carry control information and are not addressable.
- Time slots 254 and 510 are not addressable due to a hardware constraint.

At any given time, only one of the TDM busses (A or B) carries the dedicated tones, with B being the default. Entering **status port-network** will display which TDM bus is currently carrying the dedicated tones. The corresponding time slots on the other bus are normally inactive and are only used for call service, as a last resort, when every other non-control channel time slot on both busses is busy.

**Table 87: TDM Bus time slot numbers**

| TDM Bus A time slot | TDM Bus B time slot | Tone heard |
|---|---|---|
| 000 | 256 | Reorder |
| 001 | 257 | Reorder |
| 002 | 258 | Reorder |
| 003 | 259 | Reorder |

*(1 of 2)*

**Table 87: TDM Bus time slot numbers**

| TDM Bus A time slot | TDM Bus B time slot | Tone heard |
|---|---|---|
| 004 | 260 | Reorder |
| 005 | 261 | Touch Tone 1 — 697 Hz |
| 006 | 262 | Touch Tone 2 — 770 Hz |
| 007 | 263 | Touch Tone 3 — 852 Hz |
| 008 | 264 | Touch Tone 4 — 941 Hz |
| 009 | 265 | Touch Tone 5 — 1209 Hz |
| 010 | 266 | Touch Tone 6 — 1336 Hz |
| 011 | 267 | Touch Tone 7 — 1447 Hz |
| 012 | 268 | Touch Tone 8 — 1633 Hz |
| 013 | 269 | Dial Tone |
| 014 | 270 | Reorder Tone |
| 015 | 271 | Alert Tone |
| 016 | 272 | Busy Tone |
| 017 | 273 | Ringback Tone |
| 018 | 274 | Special Ringback Tone |
| 019 | 275 | 2225-Hz Tone |
| 020 | 276 | Music |
| 021 | 277 | Tone on Hold |
| 022–253 | 278–509 | Confirmation (used for calls) |
| 254 | 510 | Reorder |
| 255 | 511 | Confirmation |

***(2 of 2)***

## Out-of-Service time slot test call

This call can be used to determine whether there are any out-of-service time slots on the specified port network's TDM bus. If so, you will be connected to one. By listening to noise on the time slot and selectively removing circuit packs, you may be able to isolate the source of interference.

To place the call:

1. Dial the FAC described above and listen for dial tone.
2. Dial the port network number followed by ********.

3 Listen for one of the following tones:

| If you get... | Then... |
|---|---|
| Reorder tone | There are no out-of-service time slots on the specified port network. |
| Confirmation tone | Connection is made to an out-of-service time slot. |

4 Repeated test calls will alternate between out-of-service time slots on TDM bus A and TDM bus B.

## System tone test call

This test connects the voice terminal to a specific system tone.

To place the call:

1 Dial the FAC described above.

2 Dial the port network number followed by * and the two-digit tone identification number from the following table.

3 Listen for one of the following tones:

| If you get... | Then... |
|---|---|
| Intercept tone | The number entered is not a valid tone number. |
| Reorder tone | Inter-PN resources are not available. |
| System tone | The specified tone will be heard if it is functioning. |

**NOTE:**
For a definition of call progress tones, refer to *Overview for Avaya Communication Manager, 555-233-767*.

**Table 88: System tone identification numbers**

| Number | Description |
|---|---|
| 00 | Null tone |
| 01 | Dial tone |
| 02 | Reorder tone |
| 03 | Alert tone |
| 04 | Busy tone |
| 05 | Recall dial tone |
| 06 | Confirmation tone |

*(1 of 3)*

**Table 88: System tone identification numbers**

| Number | Description |
|---|---|
| 07 | Internal call waiting tone |
| 08 | Ringback tone |
| 09 | Special ringback tone |
| 10 | Dedicated ringback tone |
| 11 | Dedicated special ringback tone |
| 12 | Touch tone 1 |
| 13 | Touch tone 2 |
| 14 | Touch tone 3 |
| 15 | Touch tone 4 |
| 16 | Touch tone 5 |
| 17 | Touch tone 6 |
| 18 | Touch tone 7 |
| 19 | Touch tone 8 |
| 20 | Chime |
| 21 | 350 Hz |
| 22 | 440 Hz |
| 23 | 480 Hz |
| 24 | 620 Hz |
| 25 | 2025 Hz |
| 26 | 2225 Hz |
| 27 | Counter |
| 28 | External call waiting |
| 29 | Priority call waiting |
| 30 | Busy verification |
| 31 | Executive override/intrusion tone |
| 32 | Incoming call identification |
| 33 | Dial zero |
| 34 | Attendant transfer |
| 35 | Test calls |
| 36 | Recall on don’t answer |
| 37 | Audible ring |
| 38 | Camp-on recall |
| 39 | Camp-on confirmation |

*(2 of 3)*

**Table 88: System tone identification numbers**

| Number | Description |
|---|---|
| 40 | Hold recall |
| 41 | Hold confirmation |
| 42 | Zip tone |
| 43 | 2804 Hz |
| 44 | 1004 Hz (-16db) |
| 45 | 1004 Hz (0 db) |
| 46 | 404 Hz |
| 47 | Transmission test sequence 105 |
| 48 | Redirect tone |
| 49 | Voice signaling tone |
| 50 | Digital milliwatt |
| 51 | 440 Hz + 480 Hz |
| 52 | Music |
| 53 | Transmission test sequence 100 |
| 54 | Transmission test sequence 102 |
| 55 | Laboratory test tone 1 |
| 56 | Laboratory test tone 2 |
| 57 | Disable echo supervision dial tone |
| 58 | 7 seconds of answer tone |
| 59 | 4 seconds of answer tone |
| 60 | Restore music (or silence) |
| 61 | Warning tone |
| 62 | Forced music tone |
| 63 | Zip tone (first of 2 sent) |
| 64 | Incoming call ID (first of 2 sent) |
| 65 | Tone on hold |
| 66 | CO dial tone |
| 67 | Repetitive confirmation tone |
| 68 | Conference/bridging tone |
| | *(3 of 3)* |

## Media Gateway batteries

The backup batteries in the power distribution unit in the bottom of the cabinet should be replaced every four years or whenever a POWER alarm that indicates the condition of the batteries is logged. Systems with an uninterruptible power supply (UPS) may not be equipped with backup batteries.

## Media Server UPS batteries

For information about maintaining the batteries that support the S8700 Media Servers, refer to the User's Guide or other product documentation that ships with the UPS.

**PREVENTIVE MAINTENANCE LOG**

Date equipment installed: _____

| Air Filters[1] | Scheduled Date | Date Completed | Completed By | Scheduled Date | Date Completed | Completed By |
|---|---|---|---|---|---|---|
| Single-carrier cabinet | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Multicarrier cabinet | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| **Battery Packs[2]** | **Scheduled Date** | **Date Completed** | **Completed By** | **Scheduled Date** | **Date Completed** | **Completed By** |
| Single-carrier cabinet | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Multicarrier cabinet | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

1 Inspect annually; clean or replace
2 Replace every four years

Post this form with the equipment.

# Call Admission Control-Bandwidth Limitation

Call Admission Control-Bandwidth Limitation (CAC-BL) is available as a standard feature on all Linux-based platforms (S8300, S8500, and S8700). It is available in both Offer Categories A and B.

## CAC-BL description

In order to ensure Quality of Service for Voice over IP calls, there is a need to limit overall VOIP traffic on WAN links. The Call Admission Control-Bandwidth Limitation feature of Communication Manager allows the customer to specify a VOIP bandwidth limit between any pair of IP network regions, and then to deny calls that need to be carried over the WAN link that exceed that bandwidth limit.

In Communication Manager, a geographic area of high bandwidth availability, for example the LAN, or Campus, is described as an IP network region. IP network regions are generally connected to other regions by much lower bandwidth WAN facilities. Bandwidth within a single network region is considered infinite. Bandwidth between a pair of network regions is clearly finite.

Using existing IP network region administration, a customer may presently configure different voice codec sets that allow voice quality to be optimized within areas with high bandwidth inter-connectivity, or allows efficient bandwidth utilization across areas of low bandwidth inter-connectivity. The existing codec set configurations for intra and inter-region connectivity do not, however, allow explicit bandwidth limits to be set. Through existing IP trunking mechanisms, IP trunk VOIP traffic can be limited to discrete numbers of calls.

With the introduction of S8700 media servers and gateways, IP bandwidth is now also consumed for inter-gateway/ inter-PN calls, as well as IP trunk calls. Prior to the introduction of CAC-BL, there was no way at the present time to limit the bandwidth used for inter-gateway/inter-PN calls. Nor is there a way to limit the bandwidth used by IP telephones to other IP telephones or gateways. Today, when the available bandwidth is exceeded, new calls are allowed to go through, which may degrade the voice quality of the new calls and existing calls, as well.

The CAC Bandwidth Limitation feature allows explicit static bandwidth limits to be administered for all inter-region IP bearer connections. The administered bandwidth limits operate on all IP bearer connections. Bandwidth limits can be administered in terms of:

- Kbit/sec WAN facilities
- Mbit/sec WAN facilities
- Explicit number of connections
- No limit

IP network region pairs may be considered to be directly connected, or indirectly connected. Indirectly connected region pairs are connected through other directly connected region pairs. In this phase of the CAC Bandwidth Limitation feature, Communication Manager will only allow administration of one path between non-adjacent IP network regions, if needed. In many instances, the network can be modeled as though non-adjacent IP network regions are directly connected.

The CAC Bandwidth Limitation feature monitors the voice traffic bandwidth utilization across the various WAN links based on algorithms computed for each voice connection that goes over those links (using various parameters such as codec selection).

When the bandwidth limit is reached between any two regions, the feature does not allow any additional IP connections between those regions. Communication Manager re-routes the call according to existing administration:

- A coverage path
- Searching for another agent
- The next trunk group in a route pattern

The feature provides administrators with a static display of bandwidth utilization and an event log of call denials through SAT commands.

## Supported network topologies

Network topologies can be described as fully connected, hub and spoke, or a combination. All network topologies are supported, with the following two limitations:

- When more than one path exists between two network regions, the CAC-BL feature assumes that bandwidth is used across the direct path, or on a customer-specified indirect path.
- Network region pairs may have at most four intervening regions.

## Capacity constraints

The following capacity constraints apply for Release 2.0:

- Although CAC-BL itself is not limited, a maximum of 250 Network Regions may be administered for all Linux-based platforms.
- Up to 4 intervening regions can be administered in only a single indirectly-connected network path.

## CAC-BL maintenance

The Call Admission Control – Bandwidth Limitation feature provides information about the status of the bandwidth used between regions and also provides information about calls that are denied in event logs. The sections below provide details on the following:

- status ip-network-region form on page 379
- Denial events on page 381

### status ip-network-region form

The **`status ip-network-region`** form was modified to show statistics on the Call Admission Control- Bandwidth Limitation feature. The following two figures show two different command options. The first command option (an existing option) is **`status ip-network-region`** ***<n>*** and is shown in Figure 112, status ip-network-region <n>, on page 380. Each line on the form shows the connection that region ***<n>*** has to either a direct or indirect region. For the direct regions, the bandwidth and number of connections being used is shown in both the transmit and receive directions. For indirect regions, only the status of the connection is shown.

**NOTE:**
Regions not connected (either directly or indirectly) to region ***<n>*** are not shown.

**Figure 112: status ip-network-region <*n*>**

```
status ip-network-region 2

                    Inter Network Region Bandwidth Status

Src Dst   Conn     Conn     BW-limits   BW-Used (Kbits)  #-of-Connections  Denials
Rgn Rgn   Type     Stat                   Tx      Rx       Tx      Rx      Today

  2   1  direct   pass     128 Kbits       0       0       0       0        0
  2   3  indirect pass
  2   4  indirect pass
  2   5  indirect pass
```

For more details on the indirect regions, the second form of the command must be used (See Figure 113, status ip-network-region 2/3, on page 380). This command option, **`status ip-network-region <n/m>`**, shows all the bandwidth being used between regions**<*2*>** and**<*3*>**, which, in this case, includes all the intermediate regions because region**<*2*>** and region**<*3*>** are indirectly connected.

**Figure 113: status ip-network-region 2/3**

```
                    Inter Network Region Bandwidth Status

Src Dst   Conn     Conn     BW-limits   BW-Used (Kbits)  #-of-Connections  Denials
Rgn Rgn   Type     Stat                   Tx      Rx       Tx      Rx      Today

  2   1  direct   pass     128 Kbits       0       0       0       0        0
  1   3  direct   pass     256 Kbits       0       0       0       0        0
```

### *Field descriptions*

| Field | Description |
|---|---|
| Src Rgn | Source region |
| Dst Rgn | Destination region |
| Conn Type | Connection type (direct or indirect) |
| Conn Stat | Connection status (pass or fail) |
| BW-limits | Bandwidth and limits (as administered on the change ip-network-region form) |
| BW-Used (Kbits) Tx | Transmit bandwidth used (for direct connections only) |
| BW-Used (Kbits) Rx | Receive bandwidth used (for direct connections only) |
| #-of-Connections Tx | Transmit connection count (for direct connections only) |
| #-of-Connections Rx | Receive connection count (for direct connections only) |
| Denials Today | Daily denial count (for direct connections only)<br>**Note:** This log is cleared at midnight - server time |

### Denial events

Denial events can be seen by bringing up the **`display events`** form and changing the category field to denial. Several new denial events have been defined for the Call Admission Control- Bandwidth Limitation feature, and also several new denial events have been added to indicate a lack of IP resources. The new Event Types and Event Descriptions are shown in the following table

| Event Type | Event Description |
|---|---|
| 2329 | No BW, IP Media Processor <- - > IP telephone or IP trunk |
| 2330 | No BW, IP Media Processor <- - > IP Media Processor |
| 2331 | No VoIP channel, PN <- - > PN |
| 2332 | No BW, IP Media Processor <- - > G700 Media Gateway |
| 2333 | No VoIP channel, PN <- - > G700 Media Gateway |
| 2334 | No BW, G700 Media Gateway <- - > G700 Media Gateway |

## System resets

On a reset 2 or higher, all IP calls are dropped and the bandwidth usage and call counters will be cleared.

The administration of the new fields on the **`change ip-network-region`** form behave the same way during the various levels of system reset as do any other administration translations. In particular, after a serious reset (for example, reset system 3, or cold start 1), recent changes to translations will be lost if no **`save translations`** command has been executed from the SAT.

## Audits

On a time available basis, the system periodically audits the bandwidth usage and call counters to assure they are accurate.

The system performs an audit immediately upon any changes to the **`change ip-network-region`** form and updates the bandwidth usage and call counters to reflect changes in the administration of the direct or indirect routes (including changes in the intervening regions).

## CAC-BL interactions

With few exceptions, all types of calls are subjected to the CAC-BL feature for calls that need to go between network regions. Table 89, Call processing features impacted by CAC-BL, on page 382 lists call processing features impacted by CAC-BL.

For more information about Call Admission Control, see the *Administrator's Guide for Avaya Communication Manager, 555-233-506*.

**Table 89: Call processing features impacted by CAC-BL**

| | |
|---|---|
| Announcements | Media processor resources |
| Call queuing | Multi-level precedence and preemption (MLPP) |
| Call redirection | Multiple terminations |
| Call routing by trunking | Music on hold |
| Conference | RSVP |
| E911 | Shuffling |
| Firmware download to port boards | Transfer |
| Hold | |

# Analog tie trunk back-to-back testing

The TN760 circuit pack can be configured for back-to-back testing (also known as connectivity testing) by making translation and cross-connect changes. This testing configuration allows for the connection of tie trunks back-to-back in the same switch to verify the operation of tie trunk ports. The tests can be performed using either the:

- E&M mode test procedure on page 382.

  or

- Simplex mode test procedure on page 386.

## E&M mode test procedure

1. At the administration terminal, enter **list configuration trunks** to determine which ports are assigned on the Tie Trunk circuit pack.
2. Enter **display dialplan** to determine the Trunk Access Code (TAC) format.
3. Enter **display port *xxx*** for every port defined in Step 1. This lists the trunk groups of which the ports are members. For details about removing and replacing port circuit packs, see Reseating and replacing circuit packs on page 277.
4. Insert the circuit pack back into the slot.
5. Enter **display trunk *xxx p*** for each trunk group identified in Step 3. This lists the specified trunk group on the administration terminal screen and prints a hard copy on the printer. Save this data for later use.
6. Use **change trunk *xxx*** to remove every member defined by these ports from the trunk group(s).
7. Remove the Tie Trunk circuit pack from the carrier slot.
8. Set the DIP (option) switches for each of the two ports to be tested on the Tie Trunk circuit pack to “E&M mode” and “unprotected.”

9 Enter **add trunk *n*** to add a new (test) trunk group. Then enter information for the following fields:

| | |
|---|---|
| Group Type | tie |
| TAC | Use trunk access code obtained from dial plan |
| Trunk Type (in/out) | wink/wink |
| Port | Assign two of the ports from the tie trunk. |
| Mode | E&M for both ports |
| Type | Specify one port as **t1 standard** and other port as **t1 compatible**. |

Figure 114, Trunk Group form, on page 383 and Figure 115, Trunk Group form - E & M mode (Page 2 of 2), on page 384 show an example of the Trunk Group form.

**Figure 114: Trunk Group form**

```
display trunk-group 10                                        Page  1 of  5

                              TRUNK GROUP

Group Number: 10                 Group Type: tie           CDR Reports? y
  Group Name: tr 10                        COR: 1                      TAC: 110
   Direction: two-way       Outgoing Display? n        Data Restriction? n
MIS Measured? n
 Dial Access? y               Busy Threshold: 60           Night Service:
Queue Length: 0               Internal Alert? n     Incoming Destination:
   Comm Type: voice                Auth Code? n


TRUNK PARAMETERS

   Trunk Type (in/out): wink/wink    Incoming Rotary Timeout (sec): 5
    Outgoing Dial Type: tone                    Incoming Dial Type: tone
                                  Disconnect Timing (msec): 500
       Digit Treatment:                                  Digits:
          Used for DCS? n
        ACA Assignment? n

                  Baud Rate: 1200     Synchronization: async   Duplex: full
        Incoming Dial Tone? y                    Maintenance Tests? y
 Answer Supervision Timeout:                   Suppress # Outpulsing? n
```

**Figure 115: Trunk Group form - E & M mode (Page 2 of 2)**

```
                                                          Page 2 of  5

                                  TRUNK GROUP

GROUP MEMBER ASSIGNMENTS

                  Port      Name         Mode         Type    Answer Delay

               1: B1901                  E & M        t1 stan
               2: B1902                  E & M        t1 comp
               3:
               4:
               5:
               6:
               7:
               8:
               9:
              10:
              11:
              12:
              13:
              14:
              15:
```

**10** Locate the tie trunk port terminal connections at the cross-connect field. Consult the appropriate table below for either 110-type or 66-type hardware.

**11** At the cross-connect field, disconnect outside trunk facilities from the tie trunk ports and mark the disconnected wires for reconnecting the tie trunk ports to their normal configuration later. The D impact tool (AT-8762) is required to perform this step.

**12** Use jumper wires (DT 24M-Y/BL/R/G and DT 24P-W/BRN) and the D impact tool to connect wiring between the two ports assigned in Step 9 at the cross-connect field. For example, if the two ports on the analog Tie Trunk circuit pack are port 1 and 2, connect the wirings as shown below:

| Port 1 (t1 stan) (E&M) | | Port 2 (t1 comp) (E&M) |
|---|---|---|
| T1 | connected to | T12 |
| R1 | connected to | R12 |
| T11 | connected to | T2 |
| R11 | connected to | R2 |
| E1 | connected to | M2 |
| M1 | connected to | E2 |

**13** Check all wirings to verify good connections between the two test ports.

**14** Place a call from one voice terminal to another voice terminal using the tie trunk ports assigned. Dial TAC and extension. For example, if TAC of tie trunk group is 110 and station number is 5012, then dial 110 5012. If the call cannot be made, either one of these ports could be defective. There are four ports on the TN760. Try different combinations to determine defective ports.

**15** If there is a defective port on the circuit pack, try to switch to an unused port. If every port is normally used, then replace the circuit pack.

**16** Disconnect the jumpers between two ports. Then use administration terminal and trunk printouts to restore every trunk-group change to normal values.

**Table 90: Carrier lead appearances MDF**

| 110 connecting block terminals | CO Trunk TN747 | Tie Trunk TN760 |
|---|---|---|
| 1 | T1 | T1 |
| 2 | R1 | R1 |
| 3 | | T11 |
| 4 | | R11 |
| 5 | | E1 |
| 6 | | M1 |
| 7 | T2 | T2 |
| 8 | R2 | R2 |
| 9 | | T12 |
| 10 | | R12 |
| 11 | | E2 |
| 12 | | M2 |
| 13 | T3 | T3 |
| 14 | R3 | R3 |
| 15 | | T13 |
| 16 | | R13 |
| 17 | | E3 |
| 18 | | M3 |
| 19 | T4 | T4 |
| 20 | R4 | R4 |
| 21 | | T14 |
| 22 | | R14 |
| 23 | | E4 |
| 24 | | M4 |
| 25 | T5 | |

*(1 of 2)*

**Table 90: Carrier lead appearances MDF**

| 110 connecting block terminals | CO Trunk TN747 | Tie Trunk TN760 |
|---|---|---|
| 26 | R5 | |
| 27 | | |
| 28 | | |
| 29 | | |
| 30 | | |
| 31 | T6 | |
| 32 | R6 | |
| 32 | | |
| 33 | | |
| 34 | | |
| 36 | | |
| 37 | T7 | |
| 38 | R7 | |
| 39 | | |
| 40 | | |
| 41 | | |
| 42 | | |
| 43 | T8 | |
| 44 | R8 | |
| 45 | | |
| 46 | | |
| 47 | | |
| 48 | | |
| 49 | | |
| 50 | | |

*(2 of 2)*

## Simplex mode test procedure

1. Repeat steps 1 through 7 of the Table , E&M mode test procedure, on page 382.
2. Set the dip (option) switches for each of the two ports to be tested on the Tie Trunk circuit pack to simplex mode.

3 Enter **add trunk *n*** to add a new (test) trunk group. Then enter information for the following fields:

| | |
|---|---|
| Group Type | tie |
| TAC | Use trunk access code obtained from dial plan. |
| Trunk Type (in/out) | wink/wink |
| Port | Assign two of the ports from the tie trunk. |
| Mode | simplex |
| Type | type 5 |

Figure 116, Trunk Group form, page 2, on page 387 shows page 2 of the Trunk Group form.

**Figure 116: Trunk Group form, page 2**

```
                                                          Page  2 of  5

                                TRUNK GROUP


GROUP MEMBER ASSIGNMENTS

                  Port      Name         Mode         Type    Answer Delay

               1: B1901                  simplex      type 5
               2: B1902                  simplex      type 5
               3:
               4:
               5:
               6:
               7:
               8:
               9:
              10:
              11:
              12:
              13:
              14:
              15:
```

4 Locate the tie trunk port terminal connections at the cross-connect field. Consult the appropriate table above for either 110-type or 66-type hardware.

5 At the cross-connect field, disconnect outside trunk facilities from the analog tie trunk ports and mark the disconnected wires for later when the tie trunk ports are placed back into normal operation. The D impact tool (AT-8762) is required to perform this step.

6 Use jumper wires (DT 24M-Y/BL/R/G) and the D impact tool to connect wiring between the two ports assigned in Step 4 at the cross-connect field. For example, if the two ports on the analog Tie Trunk circuit pack are ports 1 and 2, connect the wirings as shown below:

| Port 1 (type 5) (simplex) | | Port 2 (type 5) (simplex) |
|---|---|---|
| T1 | connected to | T12 |
| R1 | connected to | R12 |
| T11 | connected to | T2 |
| R11 | connected to | R2 |

7 Repeat Steps 13 through 16 of the E&M mode test procedure on page 382.

# TN760E tie trunk option settings

## S8100 only

The TN760E Tie Trunk circuit pack interfaces between 4 tie trunks and the TDM bus. Two tip and ring pairs form a 4-wire analog transmission line. An E and M pair are DC signaling leads used for call setup. The E-lead receives signals from the tie trunk and the M-lead transmits signals to the tie trunk.

To choose the preferred signaling format (Table 91, Signaling Formats for TN760E, on page 388 and Table 92, Signaling type summary, on page 388), set the switches on the TN760E and administer the port using Figure 117, TN760E tie trunk circuit pack (component side) (R758183), on page 389 and Table 93, TN760E option switch settings and administration, on page 389.

**Table 91: Signaling Formats for TN760E**

| Mode | Type |
|---|---|
| E & M | Type I Standard (unprotected) |
| E & M | Type I Compatible (unprotected) |
| Protected | Type I Compatible, Type I Standard |
| Simplex | Type V |
| E & M | Type V |
| E & M | Type V Revised |

**Table 92: Signaling type summary**

| | Transmit (M-Lead) | | Receive (E-Lead) | |
|---|---|---|---|---|
| **Signaling type** | **On-hook** | **Off-hook** | **On-hook** | **Off-hook** |
| Type I Standard | ground | battery | open[1]/battery | ground |

*(1 of 2)*

**Table 92: Signaling type summary**

| | Transmit (M-Lead) | | Receive (E-Lead) | |
|---|---|---|---|---|
| **Signaling type** | **On-hook** | **Off-hook** | **On-hook** | **Off-hook** |
| Type I Compatible | open[1]/battery | ground | ground | open[1]/battery |
| Type V | open[1]/battery | ground | open | ground |
| Type V Reversed | ground | open | ground | open |

*(2 of 2)*

1 An open circuit is preferred instead of battery voltage.

**Figure 117: TN760E tie trunk circuit pack (component side) (R758183)**

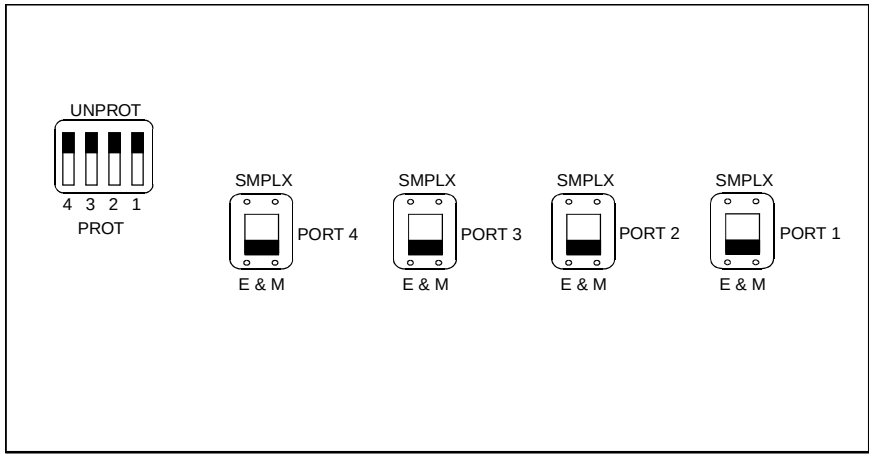



**Table 93: TN760E option switch settings and administration**

| Installation situation | | Preferred signaling format | | E&M/S MPLX switch | Prot/Unprot switch | Admin-istered port |
|---|---|---|---|---|---|---|
| **Circumstance** | **To** | **System** | **Far-End** | | | |
| Co-Located | Avaya PBX | E&M Type 1 | E&M Type 1 | E&M | Unprotected | Type 1 |
| | | Compatible | Standard | | | Compatible |
| Inter-Building | Avaya PBX | Protected Type 1 | Protected Type 1 | E&M | Protected | Type 1 |
| | | Compatible | Standard Plus | | | Compatible |
| | | | Protection | | | |
| | | | Unit | | | |
| Co-Located | Net Integrated | E&M Type 1 | Any PBX | E&M | Unprotected | Type 1 |
| | | Standard | | | | |

# TN464E/F option settings

## S8100 only

The TN464E/F DS1/E1 Interface - T1/E1 circuit pack interfaces between a 24- or 32-channel Central Office/ISDN or tie trunk and the TDM bus.

Set the switches on the circuit pack to select bit rate and impedance match. See Table 94, Option switch settings on TN464E/F, on page 390 and Figure 118, TN464E/F option settings, on page 390.

**Table 94: Option switch settings on TN464E/F**

| | |
|---|---|
| 120 Ohms | Twisted pair |
| 75 Ohms | Coaxial requiring 888B adapter |
| 32 Channel | 2.048 Mbps |
| 24 Channel | 1.544 Mbps |

**Figure 118: TN464E/F option settings**

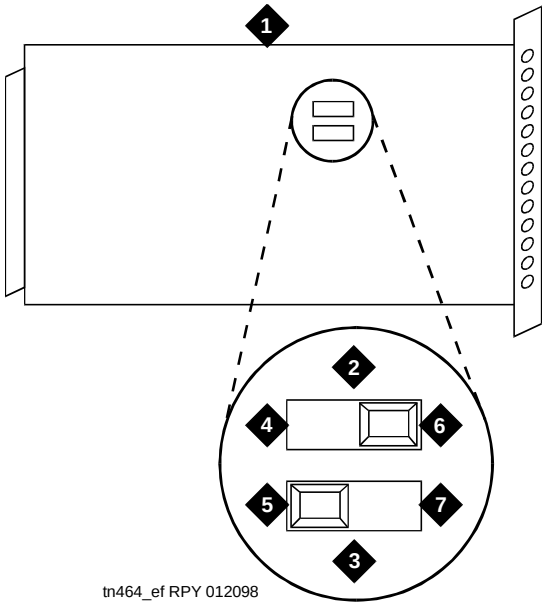



**Figure notes**

| | | | |
|---|---|---|---|
| **1** | Backplane connectors | **5** | 32 channel |
| **2** | 24/32 channel selector | **6** | 120 Ohm (shown selected) |
| **3** | 75/120 Ohm selector | **7** | 24 channel (shown selected) |
| **4** | Faceplate | | |

# Terminating Trunk Transmission testing

The Terminating Trunk Transmission (TTT) (non-interactive) feature provides for extension number access to three tone sequences that can be used for trunk transmission testing from the far end of the trunks.

The three test types should have extension numbers assigned on the Maintenance-Related System Parameters screen:

```
Test Type 100:___   Test Type 102:___   Test Type 105:___
```

Test Type 100 provides:

- 5.5 seconds of 1004-Hz tone at 0dB
- Quiet until disconnect; disconnect is forced after 1 minute.

Test Type 102 provides:

- 9 seconds of 1004-Hz tone at 0dB
- 1 second of quiet
- This cycle is repeated until disconnect; disconnect is forced after 24 hours.

Test Type 105 provides:

- 9 seconds of 1004-Hz tone at -16dB
- 1 second of quiet
- 9 seconds of 404-Hz tone at -16dB
- 1 second of quiet
- 9 seconds of 2804-Hz tone at -16dB
- 30 seconds of quiet
- ½ second of 2225-Hz test progress tone
- Approximately 5 seconds of quiet
- Forced disconnect

# Removing and restoring power

**CAUTION:**
Before powering down a carrier containing a DEFINITY AUDIX system (TN568), first power down the AUDIX unit to avoid damaging the AUDIX software. Instructions for powering down this the circuit pack are in Removing and restoring EMBEDDED AUDIX power on page 160 and in DEFINITY AUDIX documentation.

**CAUTION:**
If there is an alarm or problem suspected on the removable media do not save translations to the affected device.

## Removing and restoring power to the Media Gateway

1. For a multicarrier cabinet, set the emergency transfer switch to ON. This locks the PN in the emergency transfer mode until the trouble is cleared.
2. Depending on which type of cabinet you are powering down, do one of the following:
   - In an AC-powered multicarrier cabinet, set the circuit breaker to OFF at the power-distribution unit.
   - In a DC-powered multicarrier cabinet, turn off the DC power supply.
   - In an AC- or DC-powered single-carrier cabinet stack, turn off the power for each affected carrier individually. The ON/OFF switch is located behind the:
     — AC carrier's WP-91153 power unit
     — DC carrier's 676B power unit
3. Power is restored by reversing the action taken above.

   Restoring power will cause a restart. This process is described under EXP-PN in ABRI-PORT (ASAI ISDN-BRI Port) in *Maintenance Alarms Reference (555-245-102)*.

   If a powered-down carrier contains a 676B power unit, the 676B must have been powered down for at least 10 seconds for the unit to restart.

## Removing and restoring power from the Media Server

The media server is shut down from the media server Web interface.

To shut down a server:

1. On the Web interface main menu, under **Server**, click **Shutdown This Server**.
2. On the **Shutdown This Server** screen, choose one of the following options:
   - **Delayed**. This is the default option. When you choose this option, the system notifies all processes that the server will be shut down. The system then waits for the processes to close files and perform other clean-up activities before it shuts the server down.
   - **Immediate**. When you choose this option, the system does not wait for processes that are running to terminate normally before it shuts the server down. When you shut the server down immediately, data may be lost.
3. If you want the server to reboot after shutdown, click the check box next to **After shutdown, restart system**.
4. Click **Shutdown**.

If you selected a delayed shutdown, you will see the `shutdownproc accepted` message, indicating that the global shutdown is in progress. An immediate shutdown terminates contact with the server so no message is displayed.

To restore power to the media server:

1. Follow these steps to open the bezel door to access the power switch:
   a. Grasp the tab at each end of the hinged bezel door.
   b. Gently pull the tabs out and down to swing open the hinged bezel door.
2. Press the power switch to apply power to the server, then close the bezel door.

The lit green LED indicates that power is restored.

# Removing and restoring power on the S8100 media server

When power is removed, ***all*** S8100 features deactivate.

**NOTE:**
There is no power switch on the S8100.

There are two types of shutdown:

- "Graceful" shutdown means that all processes are told to stop, and are given time to arrive in a known, recoverable, state.
- Immediate shutdown means that all processes stop immediately without necessarily storing information.

You can command a system shutdown from the software or the hardware.

## Software shutdown

Software shutdown is performed using GAS commands at the bash shell interface. Login a Telnet session with bash as the selection.

### *Graceful shutdown*

1. Use the **shutdown system** command.

   This will close all processes, firmware, and Windows 2000. This may take several minutes, depending on what processes are running.

   The system is ready for power off when the green "OK to Remove" LED is light on the TN2314 processor circuit pack.
2. Unplug the power cord, or

   Disengage the latch on the power supply and pull it from its slot so that the backplane pins are not connected.

### *Immediate shutdown*

1. Use the **terminate system** command.

**CAUTION:**
This command will kill all processes, firmware and Windows 2000. Software may have to be re-loaded to regain operation. Use the ***shutdown*** command whenever possible.

The system is ready for power off when the green “OK Remove” LED light on the TN2314 processor circuit pack appears. (This takes about 3 minutes.)

2 Unplug the power cord, or

Disengage the latch on the power supply and pull it from its slot so that the backplane pins are not connected.

## Hardware shutdown

### *Graceful shutdown*

You will need a pen or small screwdriver for these procedures.

1 Using a small tool, press the recessed shutdown button until the “Complete” LED starts to flash on the TN2314 processor circuit pack.

The system will perform a graceful shutdown.

The system is ready for power off or removing the TN2314 circuit pack after the “Complete” LED goes to a steady green.

2 Unplug the power cord, or

Disengage the latch on the power supply and pull it from its slot so that the backplane pins are not connected.

The procedure for an immediate hardware shutdown (unplugging the system) is not recommended.

## Replacing the power supply

**WARNING:**
Ensure that the power is OFF before proceeding.

1 Pull on the latch for the 650A Power Supply.

2 Replace the power supply and secure the latch.

**NOTE:**
You will have to adjust the neon voltage after replacing the power supply. See Setting neon voltage (ring ping) on page 395 for more information.

## Restoring power

The procedures you need to restore power depend on the system configuration. Before performing these activities, refer to the appropriate procedure. Restore power as follows:

1 Plug in power cords in port cabinets first.

2 The system now goes through the rebooting process. This process takes about 3 minutes. LEDs will go through their power-up sequence. See S8100 Media Server LEDs in *Maintenance Alarms Reference (555-245-102)*.

3 The system has finished booting when the EM XFER (emergency transfer) LED goes off.

# Setting neon voltage (ring ping)

This procedure must be performed at installation and after replacement of the power supply.

> **NOTE:**
> The frequency (20, 25 or 50 Hz) is set by a switch on the power supply. Check the setting on this switch to ensure it is properly set.

## Set neon voltage to OFF

Neon voltage should be set to OFF under these conditions:

- Ringing option is set to 50 Hz. Neon voltage is not available.
- LED message lamps are used on telephones.
- No *neon* message waiting lamps on telephones.

To turn the neon voltage OFF:

1. Turn the neon voltage control to OFF (see Figure 119, Setting the neon voltage, on page 396.)

## Adjust neon voltage

The neon voltage must be adjusted under these conditions:

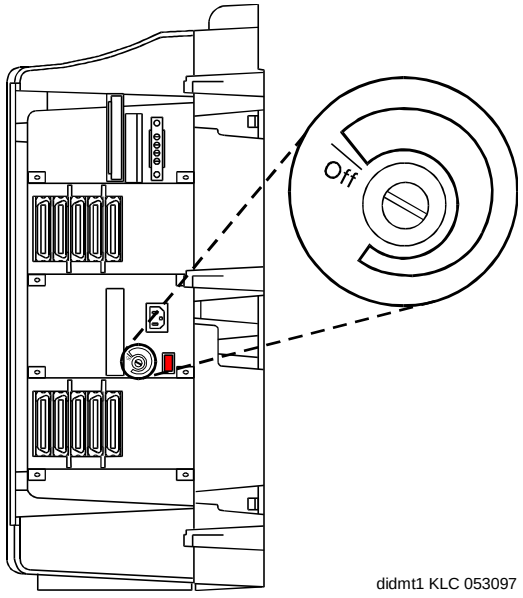
- Ringing option is set to 25 Hz. Maximum neon voltage is 120 Volts.
- Neon message waiting lamps are present on telephones.

Use the following procedure to adjust the neon voltage:

1. Call a telephone with a neon message indicator and leave a message.
2. Check for “ring ping” (single ring pulse) each time the lamp flashes (approximately every 3 seconds).
3. Adjust the neon voltage control clockwise in small increments until the ring ping stops. See Figure 119, Setting the neon voltage, on page 396.

   Ensure that the message lamp still lights when the adjustment is finished.
4. Enter **logoff** and press Enter to logoff the system and to prevent unauthorized changes to data.
5. Set the left and right doors onto the hinge pins and close the doors. The doors must be closed to prevent EMI emissions. Tighten the door screws.
6. Set the cover panel onto the right panel and secure.

**Figure 119: Setting the neon voltage**




# Removing and restoring power on the G700 Media Gateway

The G700 Media Gateway contains a detachable power cord. You can add power by plugging the power cord into the G700 receptacle, then plugging the cord into the wall outlet.

You can remove power by properly powering down the S8300 (If the G700 is equipped with an S8300), unplugging the power cord from the wall outlet, and then unplugging the power cord from the G700 receptacle.

**NOTE:**
The power supply in the G700 is not replaceable.

**NOTE:**
Auxiliary power is currently unavailable on the G700.

## S8300 Media Server shutdown operations

Depending upon the circumstances of the replacement, different S8300 server shutdown operations may be required:

1. If you are shutting down an active S8300 Media Server or a functional but inactive LSP, 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, system restart checkboxes include:
      - *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 checkbox *After Shutdown, Restart System* unchecked.

**e** Click *Shutdown.*

**2** Alternatively, you can manually initiate a shutdown process by first depressing for at least two seconds the button located next to the fourth GREEN "Ok-to-Remove" LED (specific to the S8300).

- 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.

  **NOTE:**
  The two processes described below apply to Communication Manager version 1.3 and later.

**3** If the normal shutdown procedure does 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 G700.

**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 G700 for approximately 15 seconds after the module resets.

# Automatic Transmission Measurement System

The Automatic Transmission Measurement System (ATMS) performs transmission tests on analog trunks to determine whether they are performing satisfactorily. The switch automatically originates test calls from an Originating Test Line (OTL), over the trunks to be tested, to a Terminating Trunk Line (TTL) on the switch at the far end of the trunk. Several different measurements of noise and attenuation are made and compared to administered thresholds. Test measurements can be viewed in the form of detailed or summary reports as described below.

ATMS test calls can be initiated on demand from the management terminal, or automatically by ATMS trunk test schedules. Demand tests are run with the **test analog-testcall** command which is described below.

Trunk groups can be administered to respond in different ways when a trunk fails to perform within the administered thresholds. Alarms and errors may be logged, and the trunk can be automatically busied out. When a trunk fails an unacceptable threshold twice, the system will busy it out if the trunk group is so administered and doing so will not exceed an administered limit (25, 50, 75, or 100% of the members in the group). This limit is not applied to later busyouts caused by other factors. Trunks can be manually returned to service by changing the thresholds and running a demand test or by using the release command.

## ATMS requirements

ATMS tests utilize the analog port (port number 01) on a TN771 MT circuit pack. Depending on system configuration, each PN may also contain one TN771. Multiple TN771s allow up to three concurrent test calls.

AMTS tests are designed to operate on the types of trunks found in the US, and the TN771 analog port is Mu-law companding only. The tests will not be useful in every environment.

For ATMS tests to run, several administrative prerequisites must be met. The following list shows the field entries necessary to enable testing.

**Table 95: ATMS administration**

| Form | Field | Entry/Remarks |
|---|---|---|
| System-parameters customer-options | ATMS | **y** If this field is **n**, contact your Avaya representative for a change in your license file. |
| Station | Extension | At least one TN711 analog port must be assigned. |
| | Port Number | ***UUCSS*01**, where ***UUCSS*** is the location of any TN771 |
| | Port Type COR | **105TL.** The number of a COR that has testing enabled |
| Class of Restriction | Facility Access Trunk Test | y |
| Trunk Group | Maintenance Tests ATMS Thresholds | **y** Specifies performance thresholds, the type and access number of the far-end TTL, and system response to test failures. |
| Hunt Group | | Optional, for incoming test calls. If the system has several TN771s, use the Hunt Group screen to make up a hunt group of TTLs so that one extension can be used for the whole pool. |
| ATMS Trunk Test Schedule | | Optional |

## ATMS tests

ATMS test calls can be originated either on demand or according to the ATMS test schedule. Test schedules are set up with **test-schedule** commands.

Demand test calls are originated by the **test analog-testcall** command. You can specify testing of an entire trunk group, an individual trunk, or every trunk on a single circuit pack. Trunks can be addressed by either group/member numbers or circuit pack/port locations. The type of test call, the number of the testing line on the far-end switch and various other parameters must be administered on the Trunk Group screen before the command can execute.

Normally you should invoke only the full or supervision tests. The other options are provided mainly for use in setting up an ATMS schedule. The tests that are run depend on the type of TTL at the far end to which the test call is made. The following table shows which tests are run for each type of TTL. The command syntax is as follows:

test analog-testcall
*trunkgroup#*/| *member#*| port *UUCSSpp* | board*UUCSS*
[full | supervision | no-selftest | no-return-loss | no-st-or-rl]
[*repeat#*][schedule]

## Input parameters

| Input | Description |
|---|---|
| trunk addresses | Specify a single trunk or several trunks by using **trunk**, **port**, or **board** addresses. These parameters are described in the introduction to Input parameters on page 400. If you enter a trunk-group number without a member number, every member of the group is tested. |
| full | Executes the most comprehensive test call available using the administered test set type.<br>"Full" is the default. |
| supervision | This test takes about 10 seconds and simply confirms the presence of testing capability at the far end. |
| no-selftest | Executes the full test, but skips self test sequences. This saves about 20 seconds on the type 105 transmission test and has no effect on type 100 and 102 transmission tests. |
| no-return-loss | Executes the full test but skips return loss sequences. This saves about 20 seconds on the type 105 transmission test and has no effect on type 100 or 102 transmission tests. |
| no-st-or-rl | Executes the full test but skips the self test and the return loss sequences. This saves about 40 seconds on the type 105 transmission test and has no effect on type 100 or 102 transmission tests. |
| repeat # | Specifies repeating the tests up to 99 times. The default is a single run of the tests. |
| schedule | Schedule execution of the test at a later time. This is not the same as setting up an ATMS test schedule described in ATMS tests on page 399. |

Different TTLs have different measurement capabilities, and you will need the information about specific TTL types in Table 96, Measurement capability by TTL type, on page 401, which does not include the self-test nor does it distinguish between measurements for different test tone levels.

**Table 96: Measurement capability by TTL type**

| Test | Terminating Test Line Type | | | | |
|---|---|---|---|---|---|
| | 105 Type with Return Loss | 105 Type without Return Loss | High-Level/ Low-Level Tone Source | 100 Type | 102 Type |
| Loss at 1004 Hz Far End to Near End | x | x | x | x | x |
| Loss at 1004 Hz Near End to Far End | x | x | | | |
| Loss at 404 Hz Far End to Near End | x | x | x | | |
| Loss at 404 Hz Near End to Far End | x | x | | | |
| Loss at 2804 Hz Far End to Near End | x | x | x | | |
| Loss at 2804 Hz Near End to Far End | x | x | | | |
| C-Message Noise Near End | x | x | x | x | |
| C-Message Noise Far End | x | x | | | |
| C-Notched Noise Near End | x | x | | | |
| C-Notched Noise Far End | x | x | | | |
| Return Loss[1] Near End | x | x | x | x | |
| Return Loss Far End | | | | | |

1 Return Loss includes Echo Return Loss and both high-frequency and low-frequency Singing Return Loss.

## Test call results

- If the test call successfully completes, and every trunk tests within administered thresholds for marginal and unacceptable performance, then a PASS result is returned.
- If the test aborts or fails, an error code indicating the cause is returned. The error codes are explained in the CO-TRK and TIE-TRK sections of ABRI-PORT (ASAI ISDN-BRI Port) in *Maintenance Alarms Reference (555-245-102)*.
- When the trunk is being used for call processing, the test aborts.
- When the trunk is already being tested by maintenance software, the test is queued and run when the maintenance activity finishes.

Measurement data gathered by analog testcalls can be retrieved with the **list testcalls** command as described in ATMS reports on page 403. The measurements that are made and recorded depend on the type of test that is specified and the capabilities of the far-end TTL.

Figure 120, Test results for test analog-testcall trunk 60, on page 402 shows a typical result for **test analog-testcall *trunk 60***.

**Figure 120: Test results for test analog-testcall trunk 60**

```
test analog-testcall trunk 60

                              TEST RESULTS

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

02B1901   TIE-TRK           060/001     845      PASS
02B1902   TIE-TRK           060/002     845      PASS
02B1903   TIE-TRK           060/003     845      PASS
02B1904   TIE-TRK           060/004     845      ABORT     1004
02B1905   TIE-TRK           060/005     845      PASS
02B1906   TIE-TRK           060/006     845      ABORT     1004
```

## Output fields

| Field | Description |
|---|---|
| Port | The physical location of the port supporting the trunk being tested. |
| Maintenance Name | The name of the maintenance object tested, TIE-TRK or CO-TRK. |
| Alt. Name | The trunk-group number and member number of the trunk being tested. |
| Test Number | ATMS tests are numbered 844 through 848. |
| Result | • If the test call successfully completes, and if every trunk tests within administered thresholds for marginal and unacceptable performance, then a PASS result is returned.<br>• If measurements fall outside the thresholds, the test fails. The trunks group can be administered to log errors and alarms, and to busy out the failed trunk.<br>• If the test call cannot be completed, an ABORT is returned. |
| Error Code | This numerical code indicates the reason for a failure or abort. The codes are explained in the CO-TRK and TIE-TRK sections of ABRI-PORT (ASAI ISDN-BRI Port) in *Maintenance Alarms Reference (555-245-102)*. |

# ATMS reports

The **list testcalls** command produces detailed and summary reports of measurements made by the ATMS. Measurement reports contain data on trunk signal loss, noise, singing return loss, and echo return loss, and are used to determine the quality of trunk lines. The system maintains a database with the results of the last test for each trunk. System resets clear all transmission test data, and ATMS measurements are not backed up by the MSS.

ATMS parameters are administered on the Trunk Group screen. These include thresholds for marginal and unacceptable performance. On the screen display, measurements that exceed the marginal threshold are highlighted. Measurements that are exceed the unacceptable level appear flashing, indicating unusable trunks. Trunk groups can be administered to log errors and alarms, and to busy out the failed trunk in response to such results.

The detailed report lists measurements for each trunk-group member. The summary reports lists trunk groups as a whole. The measurements that are displayed depends on what type of test, if any, was last run on the trunk, and the capabilities of the TTL on the switch at the far end of the trunk. See Test call results on page 401 for a description of the **test analog-testcall** command. A blank line indicates that no test data is available for that trunk or group.

The number of pages of each report is dependent upon the selection criteria and the number of outgoing trunks in the system. About 10 measurements can be listed on a page on the administration terminal, or about 50 measurements can be listed on a printer. By default, reports list every measurement. Filtering can be used to limit the output. For example, the report can be set up to print only failed measurements.

The syntax of the command is as follows:

list testcalls detail | summary
[port *UUCSSpp*]
[grp *group#*] [to-*grpgroup#*]
[mem *member#*] [to-*mememberl#*]
[resultresultID> | not-resultresultID]
[*count#*] [print | schedule]

## Input parameters

| Input | Description |
|---|---|
| detail | Show each measurement made for each trunk. |
| summary | Show totaled results of ATMS tests for trunk groups as a whole. |
| grp # | Show measurements for a specific trunk group. When used with **to-grp**, this option specifies the starting trunk group in a range. |
| to-grp | Show measurements for every trunk group from one up to the trunk-group number entered. When used with **grp**, this is the ending trunk group in a range. |
| mem | When used with **grp**, show measurements for a specific trunk-group member. When used with **to-mem**, this is starting trunk-group member in a range. |

*(1 of 2)*

| Input | Description |
|---|---|
| to-mem | When used with **grp**, display measurements for every trunk-group member from one up to the specified trunk-group member entered. When used with **mem**, this is the ending trunk-group member in a range. |
| port | Display measurements for the trunk assigned to a specific port circuit. |
| result | Only measurements that match the specified result are displayed. Result IDs include **pass**, **marg**, **fail**, and numerical abort codes. |
| not-result | Only measurement results that do not match the specified result are displayed. |
| count *number* | Limit the total number of records displayed. |
| print | Execute the command immediately (if resources are available) and sends output both to the screen and to a printer connected to the terminal where the command was entered. |
| schedule | Schedule a start time for the command. The command is placed in the queue and, when executed, sends the output to the system printer. |

*(2 of 2)*

## ATMS Summary Report

The ATMS Summary Report summarizes the collective results of the latest ATMS tests performed on each trunk group. By interacting with the Trunk Group screen, it highlights out-of-tolerance measurements. Marginal trunks are highlighted, and unusable trunks blink, allowing you to quickly identify out-of-tolerance or unusable trunks. Figure 121, Summary Report Screen, on page 404 shows a typical summary report.

**Figure 121: Summary Report Screen**

```
                    ATMS MEASUREMENT SUMMARY REPORT

                                Trunks   Trunks    Trunks
trk  Num   Last    Last  Passed   Failed    Failed    Trks   Trks   Busied
Grp  of    Test    Test  Transm  Marginal  Unaccept  In-    Not     Out
Num  Trks  Date    Time   Test   Threshld  Threshld  Use    Test   Trunks
1    10  10/04/91 15:15   10       0         0       0      0       0
10   10  10/04/91 15:40   10       0         0       0      0       0
20   5   10/04/91 16:00   5        0         0       0      0       0
30   30                    0        0         0              30      0
40   20  10/04/91 16:15   20       0         0       0      0       0
50   10  10/04/91 16:40   10       0         0       0      0       0
60   3   10/04/91 16:55   0        0         0       0      0       3
78   10  10/04/91 17:05   8        0         0       1      0       1
83   15  10.04/91 17:20   15       0         0       0      0       0
105  100 10/04/91 17:40   100      0         0       0      0       0
125  2   10/04/91 19:30   0        0         0       0      0       2
350  10  10/04/91 19:40   10       0         0       0      0       0
500  55  10/04/91 19:55   55       0         0       0      0       0
650  1   10/04/91 21:00   1        0         0       0      0       0
```

### Output fields

| Field | Description |
|---|---|
| Trk Grp Num | Results for each trunk group are listed by trunk-group number. Only outgoing or 2-way analog trunks are listed. |
| Num Of Trks | The number of members in the trunk group. |
| Last Test Date | The date of the oldest measurement in the trunk group. |
| Last Test Time | The time of the oldest measurement in the trunk group. |
| Trunks Passed Transm Test | The number of trunks that have passed the trunk transmission tests. |
| Trunks Failed Marginal Threshld | The number of trunks that performed outside the marginal threshold, but not the unacceptable threshold, as defined on the Trunk Group screen. |
| Trunks Failed Unaccept Threshld | The number of trunks that performed outside the unacceptable threshold, as defined on the Trunk Group screen. |
| Trks In-Use | The number of trunks that were in use at the time of testing. Abort codes for trunk-in-use are 1000 and 1004. |
| Trks Not Test | The number of trunks that were not tested due to error conditions other than trunk-in-use. Abort codes are given in the detailed report. |
| Busied Out Trunks | The number of trunks that were busied out in response to test failures. These may be caused by hardware problems, incorrect threshold values, and so on. |

## ATMS detail report

This report is divided into two sections. The upper section lists the trunk group, trunk type, trunk vendor, TTL type, and the user-defined threshold values administered on page 4 of the Trunk Group screen (Figure 122, ATMS detail report, on page 406). The lower section lists the most recent set of measurements for each member of the trunk group selected for the report. Measurements that exceed the marginal threshold, but not the unacceptable threshold, are highlighted. Measurements that exceed the unacceptable threshold blink, identifying unusable trunks. When a marginal or unacceptable measurement is found, scan the top section to find out how far the measurement deviates from its defined threshold.

**Figure 122: ATMS detail report**

```
                          ATMS TRUNK MEASUREMENTS
Group: 78  Type: co     Vendor: AT&T                TTL Type: 105-w-rl

THRESHOLD VALUES
                                    Loss dev at
                      1004Hz-loss  404Hz 2804Hz  C-msg C-ntch    SRL  SRL
                        Min  Max    -  +  -  +   Noise Noise     LO   HI  ERL
             Marginal    -2   21     9  9  9  9     55    74       0    0   0
         Unacceptable    -2   21     9  9  9  9     55    74       0    0   0
Trk Test  Test  Test -16dBm OdBm
Mem Date  Time  Rslt FE NE  FE NE  FE NE FE NE  FE NE FE NE  FE NE FE NE FE NE
1   10/04 14:25 pass 7  7   7  7   -2 -2 7  7   15 28 34 34  8  16 11 16 11 17
2   10/04 14:26 1920
3   10/04 14:27 1000
4   10/04 14:28 pass 7  7   7  7   -2 -2 7  7   15 29 38 34  8  16 11 15 11 16
5   10/04 14:29 pass 7  7   7  7   -2 -2 6  6   15 35 34 34  8  6  9  6  10 7
6   10/04 14:30 pass 7  7   7  7   -2 -2 6  6   15 26 34 34  8  16 9  13 10 16
7   10/04 14:31 pass 7  7   7  7   -2 -2 7  7   15 30 34 34  8  16 9  11 10 13
8   10/04 14:32 pass 6  6   6  6   -2 -2 6  6   15 25 34 34  10 17 11 16 12 17
9   10/04 14:33 pass 6  6   7  7   -1 -1 7  7   15 25 34 34  8  15 9  13 10 16
10  10/04 14:34 pass 6  6   7  6   -1 -1 7  7   15 36 34 35  8  6  9  6  10 7
```

## Output fields—ATMS detail report

Measurements are made in both directions, near to far end, and far to near end. For each measurement, there are two columns on the lower part of the report, “NE” for near end, and “FE” for far end. These refer to the destination end for that measurement.

| Field | Description |
|---|---|
| Group | The trunk-group number selected |
| Type | The trunk-group type |
| Vendor | The vendor of this trunk group |
| TTL Type | The type of terminating test line on the switch at the far end of the trunk to which the test call was made |
| Threshold Values | The list of marginal and unacceptable threshold values for each type of measurement as defined on the Trunk Group screen |
| Trk Mem | The trunk-group member number |
| Test Date | The month and day this trunk was last tested |
| Test Time | The time of day this trunk was last tested |

*(1 of 2)*

| Field | Description |
|---|---|
| Tst Rslt | The results of the trunk transmission test as follows:<br>• pass: the test call completed successfully and trunk performance was satisfactory.<br>• marg: trunk measurements exceeded the marginal threshold, but not the unacceptable.<br>• fail: trunk measurements exceeded the unacceptable threshold.<br>• xxxx: a numerical error code indicates the reason for an aborted test call. The codes are explained in the CO-TRK and TIE-TRK sections of ABRI-PORT (ASAI ISDN-BRI Port) in *Maintenance Alarms Reference (555-245-102)*.<br>• blank: indicates that no measurements have been made on this trunk since the database was last initialized. |
| 1004Hz-loss Min | Far-to-near and near-to-far measurements of 1004-Hz loss from low-level tone. |
| 1004Hz-loss Max | Far-to-near and near-to-far measurements of 1004-Hz loss at 0 dBm. |
| Loss dev at 404Hz | These low-frequency transmission tests measure maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements. |
| Loss dev at 2804Hz | These high-frequency transmission tests measure maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements. |
| C-msg Noise | Maximum interference noise on a voice terminal within the voice-band frequency range (500 to 2500 Hz). The measurement ranges from 15 to 55 dBrnC (decibels above reference noise). |
| C-ntch Noise | Maximum signal-dependent noise interference on a line between 34 and 74 dBrnC. |
| SRL-LO | Singing return loss from 0 to 40 dB between the sum of the circuit (repeater) gains and the sum of the circuit losses. SRL-LO occurs most often in the frequency range of 200 to 500 Hz. |
| SRL-HI | Singing return loss from 0 to 40 dB between the sum of the circuit (repeater) gains on a circuit and the sum of the circuit losses. SRL-HI occurs most often in the frequency range of 2500 to 3200 Hz. |
| ERL | Echo return loss from 0 to 40 dB between the level of signal strength transmitted and the level of signal strength reflected. ERL occurs most often in the frequency range of 500 to 2500 Hz. |

*(2 of 2)*

## ATMS measurement analysis

ATMS compares the results of the test measurements with threshold values to identify trunks that are out of tolerance or unusable. Once a defective circuit has been pinpointed, a proper analysis must be made to determine the appropriate action to take on the facility failures. Although there is no “right” procedure for every situation, the following items will help in troubleshooting problems:

- If a circuit fails an ATMS transmission test, it does not necessarily mean the trouble is in the facility itself. The problem could be caused by a faulty test line, bad switch path, or a variety of other reasons.
- If a circuit fails a transmission test but successfully passes a supervision test, some of the items mentioned above are probably not at fault, since proper call routing and circuit continuity are required for successful of a supervision test.
- If several circuits in the same group are failing, this could indicate the failure of some common equipment (such as a carrier system, test line, or cable) or erroneous information in the threshold tables.
- When a test call can be successfully made, but not completed, either the OTL or TTL is probably defective. For this failure type, further ATMS testing might be seriously impaired, but the system is not otherwise affected.
- If a test call cannot be successfully made, the wrong number might have been dialed, the far-end device might be busy, the far-end device is defective, or there is a serious trunk failure obstructing the call.

# Setting G700 synchronization

If the Avaya G700 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 G700. In so doing, clock sync signals from the Central Office (CO) are used by the MM710 to synchronize all operations of the G700. 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 Processor (MGP) command line interface (CLI). The command (in *configure* mode) **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

For the MM720 BRI Media Module, <portID> is formed by combining the mmID of the MM to the 2-digit port number of the BRI port.

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”, and, 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”.

Use the following procedure:

1. Login at the **Welcome to Media Gateway Server** menu.
   You are now logged-in at the Supervisor level on the Media Gateway Processor. The prompt appears as **MG-mmm-1(super)**>, where **mmm** is the administered G700 Media Gateway number in the network.
2. Type **configure** to access the configuration prompt.
   The prompt will change to indicate that you are in configuration mode. In the configuration mode, you may use the **set** commands.
3. At the prompt, type **set sync interface primary <mmid>**.
   The MM710 Media Module is now configured as the primary clock synchronization source for the G700 Media Gateway.
4. At the prompt, type **set syn sou pri**.
5. If the G700 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 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 G700 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 G700 synchronization sources

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

**NOTE:**
Unless otherwise indicated, the following commands issue from the G700 MGP CLI.

**Table 97: mgp-001-1(configure)# 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 98: mgp-001-1(configure)# set sync interface primary v4**
**mgp-001-1(configure)# 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<br>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 issued. | | | |

**Table 99: mgp-001-1(configure)# set sync source primary**
**mgp-001-1(configure)# 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 issued from the SAT CLI, and not from the MGP CLI.

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

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

The results from the above command are shown in Table 100:

**Table 100: TEST RESULTS**

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

If a secondary is similarly provisioned:

**Table 101: mgp-001-1(configure)# set sync interface secondary v3**
**mgp-001-1(configure)# show sync timing**

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

To activate the secondary, the following is similarly done:

**Table 102: mgp-001-1(configure)# set sync source secondary**
**mgp-001-1(configure)# 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 local the following is done:

**Table 103: mgp-001-1(configure)# set sync source local**
**mgp-001-1(configure)# 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, the following is done:

**Table 104: mgp-001-1(configure)# set sync source primary**
**mgp-001-1(configure)# 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 were removed, then the secondary becomes active and the primary reports a failure.

**Table 105: mgp-001-1(configure)# 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 these documents for troubleshooting details and error codes, as well as the phone administration information:

- *4606 IP Telephone User's Guide, 555-233-775*
- *4624 IP Telephone User's Guide, 555-233-776*
- *4612 IP Telephone User's Guide, 555-233-777*

The Avaya 4600-Series IP Telephones are relatively trouble-free. Table 106, IP Telephone problems and solutions, on page 413 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 as follows:

- Phone does not activate after connecting it the first time
- Phone does not activate 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
- All other IP Phone problems

**Table 106: IP Telephone problems and solutions**

| 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 causes. |
| Characters do not appear on the Display screen | See "*Phone does not activate after connecting it the first time*" above.<br><br>Check the power source to be sure your telephone is receiving power.<br><br>Check all lines into the phone to be sure it is properly connected.<br><br>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.<br><br>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. |

***(1 of 2)***

**Table 106: IP Telephone problems and solutions**

| Problem/Symptom | Suggested solution |
|---|---|
| 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.<br><br>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.<br><br>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.<br><br>Reset or power cycle the phone.<br><br>See your Telephone System Administrator if the above steps do not produce the desired result.<br><br>Check the status of the VoIP board. |
| Echo, noise or static when using a headset; handset operation works properly | Check the headset connection.<br><br>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.<br><br>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.<br><br>Set your ringer volume to a higher level using the Up/Down Volume keys.<br><br>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.<br><br>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. |

***(2 of 2)***

# Resetting and power cycling IP Telephones

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

## Resetting an IP Telephone

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 107, Resetting the IP Telephone, on page 415:

**Table 107: Resetting the IP Telephone**

| If you want to... | Then... |
|---|---|
| Reset the phone without resetting any assigned values | Press * (asterisk).<br>A confirmation tone sounds and the display prompts "Restart phone? * = no # = yes." |
| Reset the phone and any previously assigned (programmed) values<br>(Use this option only if your phone has programmed, static values) | Press # (the pound key)<br>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. At the switch, incoming IP endpoint registration requests are rejected when processor occupancy is at or above 85%. This event is recorded in the software events log. No alarms are generated for this event.

## Power cycling an IP Telephone

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

### *To power cycle an IP Telephone*

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 System Administrator.

# Index

## Numerics



## A



## B

## C



## D

## E



## F



## G



## H

## I



## J



## K



## L

## M



## N

## O



## P



## Q



## R

## S



## T

## U



## V



## W

## X