Maintenance Procedures for Avaya Communication Manager 3.1.x, Media Gateways and Servers

03-300432
Issue 2.1
June 2006

© 2006 Avaya Inc.
All Rights Reserved.

Notice

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

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

http://www.avaya.com/support

Copyright

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

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Contents

About this book 13

Overview 13

Document set 13

Equipment/platforms 13

Audience 14

Downloading this book and updates from the Web 15

Downloading this book 15

Safety and security-alert labels 15

Safety precautions 16

Electrostatic discharge 16

Suppressing alarm origination 17

Related resources 17

Technical assistance 19

Within the United States 19

International 19

Trademarks 19

Sending us comments 20

How to use this document 20

Organization 21

Conventions used in this document 22

Useful terms 23

Chapter 1: Maintenance strategy 25

Maintenance Objects 25

Maintenance testing 26

Background testing 27

Demand testing 28

Alarm and error reporting 28

Alarm and error logs 29

Alarm reporting 30

Alarm reporting options 31

Power interruptions 34

Nominal power holdover 34

Power interruption effects 35

External alarm leads 35

Protocols 36

OSI layers 36

Usage 38

Protocol states 40

Connectivity rules . . . 41
Signaling . . . 42
Disconnect supervision . . . 42
Transmission characteristics . . . 44
Service codes . . . 48
Facility Interface Codes . . . 48
Multimedia Interface (MMI) . . . 49
S8300 and G700 maintenance strategy . . . 50
Removing and restoring EMBEDDED AUDIX power . . . 51
Media Module maintenance . . . 52
Access to the G700 Media Gateway and S8300 Media Server . . . 53
S8300 Media Server Web interface . . . 53
G700 Media Gateway Processor CLI . . . 54
Layer 2 Switching Processor CLI . . . 54
G700 server-controlled maintenance . . . 54
DEFINITY equivalent elements . . . 54
Capacity constraints and feature limitations . . . 56
Testing . . . 62
Maintenance features for the G700 . . . 66

Chapter 2: Access and login procedures . . . 69

S8300 connections . . . 69
Laptop settings and connections . . . 70
Secure access . . . 83
Secure Shell and Secure FTP . . . 83
Secure Copy . . . 88
Administration . . . 89
Login methods . . . 90
Logging in using a telnet session on your laptop . . . 90
Logging in to the S8300 Web interface from your laptop . . . 91
Logging in to Communication Manager (SAT screens) . . . 91
Logging in to the Layer-2 switching processor . . . 92
Navigating the Command Line Interface . . . 94

Chapter 3: S8400 Maintenance Processor Complex . . . 97

Login administration . . . 97
Creating a remote (modem) login . . . 98
Creating a local (MPC) login . . . 98
Changing a local login to a remote login . . . 99

Changing a remote login to a local login . . . 99
Removing a MPC login . . . 99
Connecting and logging in to the MPC . . . 99
Connecting through a Web browser . . . 99
Connecting locally through SSH . . . 101
Connecting remotely through SSH . . . 101
Connecting remotely through a Web browser . . . 102
MPC Web interface . . . 104
Home page . . . 104
Log . . . 106
Processor Complex . . . 107
Management Complex . . . 108
System Blade / Overall System Health . . . 111
Power / Reset . . . 115
Inventory Data . . . 117
Verifying the internal link . . . 118
Disabling the boot timer . . . 118
Disabling the boot timer through the Web interface . . . 118
Disabling the boot timeout using Linux commands . . . 119
Password protection . . . 120
Updating the MPC firmware . . . 121
Determining the latest firmware version . . . 121
Downloading new firmware to the staging area . . . 122
Accessing the server . . . 122
Copying and installing MPC firmware to the server . . . 123

Chapter 4: Server initialization, recovery, and resets . . . 125

S8700 Initialization . . . 125
Active server's initialization . . . 126
Standby server's initialization . . . 127
Automatic trace-route . . . 127
Hardware/software requirements . . . 128
Monitored links . . . 128
Configurations . . . 129
Administration . . . 129
Command results . . . 130
Conditions and interactions . . . 135
Network recovery . . . 137
Connection Preserving Failover/Failback . . . 138
Modem Dial Backup . . . 149

H.248 server-to-gateway Link Recovery . . . 149
H.323 gateway-to-endpoint Link Recovery . . . 159
Auto Fallback to Primary . . . 174
Local Survivable Processor (LSP) . . . 175
Enterprise Survivable Server (ESS) . . . 176
Standard Local Survivability (SLS) . . . 178
Prerequisites . . . 179
Licensing . . . 180
Detailed description . . . 180
Limited call processing in survivable mode . . . 181
Complete provisioning data . . . 182
Communication Manager data . . . 184
PIM data . . . 184
How the G250 enters survivable mode . . . 185
SLS states . . . 186
Direct Inward Dialing (SLS) . . . 187
Multiple call appearances . . . 188
Hold (SLS) . . . 188
Call Transfer (SLS) . . . 190
Contact closure . . . 192
IP Softphone shared administrative identity . . . 195
Gateway translation conversion . . . 196
Preventing PIM updates . . . 196
Emergency Transfer in survivable mode . . . 197
SLS logging activities . . . 198
SLS administration procedures . . . 200
Manually configuring the SLS data on the media gateway . . . 208
System resets . . . 219
Reset Level 1 (Warm Restart) . . . 219
Reset Level 2 (Cold-2 Restart) . . . 220
Reset Level 3 (Communication Manager reboot) . . . 221
Reset Level 4 . . . 222
Reset Level 5 (Extended Communication Manager reboot) . . . 223
S8300/G700 system reset . . . 223

Chapter 5: General troubleshooting . . . 225

Introduction . . . 225
Alarm and event log . . . 226
Commonly-accessed directories and files on Linux servers . . . 228

Knowing when there is a problem . . . 230
Equipment indicators . . . 231
User-reported problems . . . 231
Status reports and activity tracing . . . 234
Viewing the alarm and event logs . . . 236
Viewing the Maintenance Web page log . . . 237
Viewing the SAT log . . . 237
Viewing the Web interface logs . . . 241
Interpreting the Communication Manager report . . . 243
Diagnosing the problem . . . 244
Repairing or escalating the problem . . . 245

Chapter 6: Troubleshooting IP telephony . . . 249

Troubleshooting the TN2302AP and TN799DP circuit packs . . . 250
Troubleshooting H.323 trunks . . . 250
Signaling group assignments . . . 250
No MedPro resources available . . . 251
CLAN sharing . . . 252
Troubleshooting problems with shuffling and hairpinning . . . 252
Reviewing a station's IP connection status . . . 253
Reviewing a trunk's IP connection status . . . 254
Reviewing the IP network region status . . . 255
Displaying failed IP network region connections . . . 256
Testing failed IP network regions . . . 256
Conditions and solutions . . . 257
Troubleshooting Avaya IP telephones . . . 260
Troubleshooting IP Softphone . . . 260
Telecommuter use of phone lines . . . 260
iClarity audio level adjustments . . . 261
No Dial Tone . . . 261
Terminology . . . 261
Symptom resolution procedure . . . 262
Talk path . . . 265
Symptom resolution procedure . . . 265
Poor audio quality . . . 269
Dropped calls . . . 273
Symptom resolution procedure . . . 273
Echo . . . 274

Chapter 7: Troubleshooting the S8400 Maintenance Processor Complex (MPC) . . . 275
MPC channel traffic . . . 275
Detecting the MPC . . . 275
Testing the internal LAN . . . 276
MPC diagnostics . . . 276
MPC configuration diagnostics . . . 277
Testing the MPC through SSH . . . 278
Testing HPI . . . 278
Testing NTP . . . 281
Rebooting the MPC . . . 282

Chapter 8: Troubleshooting trunks . . . 283
Troubleshooting trunks with Automatic Circuit Assurance . . . 283
Using Busy Verification of Terminals and Trunks . . . 284
Troubleshooting ISDN-PRI . . . 284
Troubleshooting ISDN-PRI endpoints (wideband) . . . 286
Troubleshooting ISDN-BRI / ASAI . . . 288
Troubleshooting ISDN-PRI test calls . . . 291
Synchronous method . . . 292
Asynchronous method . . . 293
Troubleshooting the outgoing ISDN-testcall command . . . 294

Chapter 9: Other troubleshooting . . . 295
Troubleshooting duplicated servers . . . 295
Determining the time of a spontaneous interchange . . . 296
Fiber link fault isolation . . . 296
Troubleshooting SNI/EI links with manual loop-back . . . 301
Isolating fiber faults with loopback tests . . . 302
Troubleshooting ATM . . . 304
Initial LED inspection . . . 305
A500 switch diagnostics . . . 307
ATM administration . . . 309
A500 administration . . . 314
TN230X circuit pack(s) . . . 318
Physical layer . . . 321
SONET layer . . . 323
Q.SAAL (data link) layer . . . 325
Q.93B (network) layer . . . 326
ATM call control . . . 329

CaPro layer . . . 329
Unusual ATM trouble conditions . . . 333

Chapter 10: Communication Manager / Linux logs and Tripwire reports . . . 337

Detecting system intrusion . . . 337
Accessing system logs through the Web interface . . . 338
Select Log Types . . . 339
Select a View . . . 347
Select Event Range . . . 349
Display Format . . . 349
Interpreting the log entries . . . 350
Tripwire . . . 350
Enabling Tripwire . . . 351
Tripwire Commands . . . 352
Reclaiming a compromised system . . . 354

Chapter 11: Backup procedures . . . 355

S8500 and S8700 backup procedures . . . 355
S8300 backup procedures . . . 358
Shutting down AUDIX . . . 358
Backing up data files . . . 359
Backup History . . . 362
Schedule Backup . . . 363
Adding or changing a scheduled backup . . . 363
Removing a scheduled backup . . . 366
Backup Logs . . . 367
Preview Data . . . 369
View/Restore Data . . . 369
Restore History . . . 371
Format PC Card . . . 372

Chapter 12: Component replacement . . . 375

Variable-speed fans . . . 375
Replacing variable-speed fans . . . 376
Replacing the fan power filter . . . 376
Replacing the temperature sensor . . . 377
Reseating and replacing circuit packs . . . 378
Special procedures . . . 378

CMC1 component maintenance . . . 379
Replacing fans and air filters (CMC1) . . . 379
S8300 component maintenance . . . 380
S8400 component maintenance . . . 381
S8500 component maintenance . . . 381
S8700 component maintenance . . . 381
G650 component maintenance . . . 382
G650 fan removal/replacement . . . 382
Replacing a BIU or rectifier . . . 383

Chapter 13: Packet and serial bus maintenance . . . 385

Isolating and repairing packet-bus faults . . . 385
Remote versus on-site maintenance . . . 386
What is the packet bus? . . . 387
Packet-Bus faults . . . 387
Packet bus connectivity . . . 388
Circuit packs that use the packet bus . . . 389
Effects of circuit-pack failures on the packet bus . . . 390
Packet bus maintenance . . . 391
General fault correction procedures . . . 393
Maintenance/Test circuit pack (TN771D) . . . 394
Packet bus fault isolation flowchart . . . 402
Troubleshooting procedures . . . 409
Systems with nonduplicated SPEs . . . 412
G650 Serial Bus fault detection and isolation . . . 415
Procedure 1 . . . 417
Procedure 2 . . . 418

Chapter 14: Additional maintenance procedures . . . 421

SBS maintenance . . . 421
No Media Processor issues . . . 421
Signaling group maintenance . . . 422
SBS trunk service states . . . 422
Trunk member status . . . 423
SBS extension status . . . 423
Finding the parties Involved in an SBS Call . . . 423
Errors and denial events . . . 425
System resets . . . 426
Upgrades . . . 426
Duplication interactions . . . 426

Traffic measurement . . . 426
Re-using an IPSI circuit pack . . . 427
Moving from dynamic to static addressing . . . 428
Moving from static to dynamic addressing . . . 430
Updating software, firmware, and BIOS . . . 431
DS1 CPE loopback jack (T1 only) . . . 432
Loopback Jack installation . . . 433
Administration . . . 434
DS1 span test . . . 434
Loopback Jack fault isolation procedures . . . 437
Configurations using fiber multiplexers . . . 444
Facility test calls . . . 445
Trunk test call . . . 446
DS0 Loop-Around test call . . . 447
DTMR test call . . . 448
TDM bus time slot test call . . . 449
Out-of-Service time slot test call . . . 451
System tone test call . . . 452
Media Gateway batteries . . . 455
Media Server UPS batteries . . . 455
Call Admission Control-Bandwidth Limitation . . . 456
CAC-BL description . . . 457
Supported network topologies . . . 458
Capacity constraints . . . 458
CAC-BL maintenance . . . 458
System resets . . . 460
Audits . . . 460
CAC-BL interactions . . . 461
Analog tie trunk back-to-back testing . . . 461
E&M mode test procedure . . . 462
Simplex mode test procedure . . . 468
TN760E tie trunk option settings . . . 470
TN464E/F option settings . . . 472
Terminating Trunk Transmission testing . . . 473
Removing and restoring power . . . 474
Removing and restoring power to the G250 / G350 Media Gateways . . . 474
Removing / restoring power: S8700 Series Media Servers . . . 475
Setting neon voltage (ring ping) . . . 478
Set neon voltage to OFF . . . 478

Adjust neon voltage 478
Removing and restoring power on the G700 Media Gateway 479
Automatic Transmission Measurement System 481
ATMS requirements 482
ATMS tests 483
ATMS reports 487
ATMS summary report 489
ATMS detail report 490
ATMS measurement analysis 492
Setting G700 synchronization 493
Viewing G700 synchronization sources 495
IP Telephones 498
Resetting and power cycling IP Telephones 500

Index 503

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.

Document set

Although this maintenance book is published separately, it is part of a set:

- *Maintenance Alarms Reference (03-300430)* (formerly 03-300190, 555-245-102)
- *Maintenance Commands Reference (03-300431)* (formerly 03-300191, 555-245-101)
- *Maintenance Procedures (03-300432)* (formerly 03-300192, 555-245-103)

Equipment/platforms

This book contains information about the following equipment/platforms

- Avaya S8700/S8710 Media Servers
- Avaya S8500 Media Servers
- Avaya S8400 Media Servers
- Avaya S8300 Media Servers
- Avaya G700/G650/G350/G250/MCC/SCC Media Gateways

It does not contain information about

- DEFINITY G3R (see 555-233-117: *Maintenance for DEFINITY R Servers* or 555-233-142: *Maintenance for Avaya S8700 Media Servers with G600 Media Gateway*)
- DEFINITY SI (see 555-233-119: *Maintenance for DEFINITY SI Servers* or 555-233-143: *Avaya S8700 Media Servers with MCC1/SCC1*)
- Avaya S8100 Media Server (see 555-233-123: *Maintenance for DEFINITY CSI Servers*)
- IBM eServer BladeCenter HS20 Type 8832
- G150/G250/G350 Media Gateways

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 Support 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. Click on the **FIND DOCUMENTATION and DOWNLOADS by PRODUCT NAME** link.

   The system displays the **Find Documentation and Downloads by Product Name** page.
3. Select from the numerically and alphabetically sorted documents on the page.

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

Before attempting repair on any equipment observe the prescribed safety precautions, thus avoiding unnecessary damage to the equipment and disruption of service. The items on this list should be a regular part of your safety 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. See Electrostatic discharge for more information.
- When you log on with Avaya Site Administration alarm notification is normally disabled. See Suppressing alarm origination for more information. Log off Avaya Site Administration as you leave the system.
- Always busyout 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 51, on the circuit pack, and in EMBEDDED AUDIX documentation.

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, touch 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:
Humans collect potentially damaging amounts of static electricity from many ordinary activities. The smallest amount of ESD humans can feel is far above the threshold of damage to a sensitive component or service disruption.

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.

Related resources

Table 1 lists additional documentation is referenced within this document.

Table 1: Additional document resources *1 of 3*

Document	Number
Hardware Description and Reference for Avaya Communication Manager, 555-245-207	555-245-207
Administrator Guide for Avaya Communication Manager, 03-300509	03-300509
	1 of 3

Table 1: Additional document resources *2 of 3*

Document	Number
Overview for Avaya Communication Manager, 03-300468	03-300468
Installing and Upgrading 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 Application Solutions-IP Telephony Deployment Guide, 555-245-600	555-245-600
Using the Avaya Enterprise Survivable Servers (ESS), 03-300428	03-300428
Avaya C360 Manager User Guide	N/A
Avaya P333T User's Guide	N/A
Quick Start for Hardware Installation: Avaya S8700 Media Server, 555-245-703	555-245-703
Installing and Configuration an Avaya S8700 Series Media Server, 03-300145, and Installing the Avaya G650 Media Gateway, 03-300685	03-300145 03-300685
Quick Start for Hardware Installation: Avaya S8500 Media Server, 555-245-701	555-245-701
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 Aids for Field Replacements (FRUs) for the Avaya S8300 Media Server with the G700 Media Gateway, 03-300538	03-300538
Job Aids for Field Replacements (FRUs) for the Avaya S8400 Media Server, 03-300623	03-300623
Job Aids for Field Replacements (FRUs) for the Avaya S8500 Media Server, 03-300529	03-300529
Job Aids for Field Replacements (FRUs) for the Avaya S8700 Series Media Servers, 03-300530	03-300530
Job Aid: Upgrading Firmware on the BIOS—Avaya S8500 Media Server, 03-300411	03-300411
The Avaya RSA Users' Guide, 555-245-702	555-245-702
	2 of 3

Table 1: Additional document resources *3 of 3*

Document	Number
Upgrading, Migrating, and Converting Media Servers and Gateways, 03-300412	03-300412
Job Aid: Firmware Download Procedure for the G700 Media Gateway, 555-245-758	555-245-758
	3 of 3

Technical assistance

Avaya provides the following resources for technical assistance.

Within the United States

For help with:

- Feature administration and system applications, call Avaya Technical Consulting Support 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

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

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

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 (03-300430)* generally addresses these needs. Certain complex elements of the system require a more comprehensive approach. Special procedures for these elements appear in Chapter 5: General 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: S8400 Maintenance Processor Complex, describes the remote maintenance functions of the MPC on the Avaya S8400 Media Server.
- Chapter 4: 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 5: General 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 6: Troubleshooting IP telephony, includes specific troubleshooting techniques for IP system configurations.
- Chapter 7: Troubleshooting the S8400 Maintenance Processor Complex (MPC), describes troubleshooting procedures for the remote maintenance MPC on the Avaya S8400 Media Server.
- Chapter 8: Troubleshooting trunks, discusses troubleshooting trunk-related problems.
- Chapter 9: Other troubleshooting, includes troubleshooting duplicated servers, fiber links, and ATM.
- Chapter 10: Communication Manager / Linux logs and Tripwire reports, describes several log types, the entries in them, and their interpretation. Tripwire monitoring of platform and Communication Manager files and how to reclaim a compromised system are also discussed.
- Chapter 11: Backup procedures, describes how to back up Communication Manager and Linux server files through the Maintenance Web interface.
- Chapter 12: Component replacement, describes preventive maintenance, procedures for replacing fans, filters, hard drives, servers, and interfaces.
- Chapter 13: Packet and serial bus maintenance, describes fault isolation and repair procedures for the packet bus and the G650 serial bus.
- Chapter 14: Additional maintenance procedures, describes component, trunk, and 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 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	**S8700 | 8710**: Ensure that the duplication link is securely connected.
	• Lines set apart extended information intended for a specific system component.	**G700** Ensure that Media Module is securely seated and latched in the carrier.
SAT and Linux commands	• Constant-width bold for **`commands`** • Square brackets **`[ ]`** around optional parameters • "Or" sign | between exclusive choices • Constant-width bold italic for ***`variables`***	**`refresh ip-route [all | location]`** **`display trunk group grp# / mbr#`**
Interface input and output	• Bold for **input, field names**, and **output** (screen displays and messages)	Set the **Save Translation** field to **daily**. The message **Command successfully completed** appears.
Web interface	• Bold for **menu selections, tabs, buttons,** and **field names** • Right arrow **>** to separate a sequence of menu selections	Select **Alarms and Notification**, the appropriate alarm, and then click **Clear**. Select **Diagnostics > View System Logs**, then click **Watchdog Logs**.

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 TN790B 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 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 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	i960 Processor C360 Stack Processor

Chapter 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 (03-300430)*. This chapter includes the following topics:

- Maintenance Objects on page 25
- Alarm and error reporting on page 28
- Power interruptions on page 34
- Signaling on page 42
- Service codes on page 48
- Facility Interface Codes on page 48
- Multimedia Interface (MMI) on page 49
- S8300 and G700 maintenance strategy on page 50
- G700 server-controlled maintenance on page 54

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 (03-300430)* 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 co-reside 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 | 8710** 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 (03-300430)*.

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)
LIC-ERR	10
MED-GTWY	10
NR-CONN	10
POWER	10
SPE-SELEC	10
STBY-SPE	10
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.

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 (03-300431)*, and the maintenance objects in *Maintenance Alarms Reference (03-300430)*.

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 as shown in Table 4.

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:

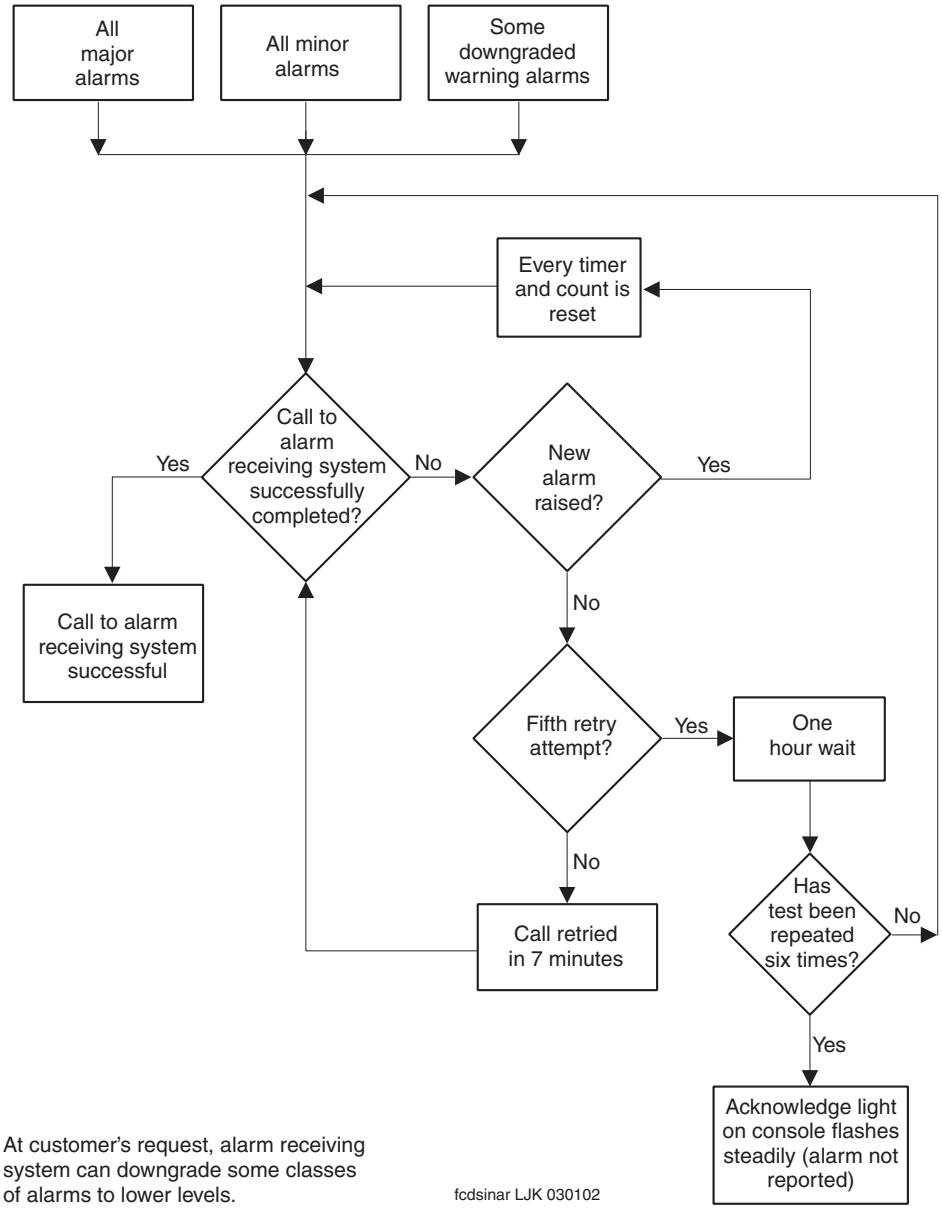
To determine the actual level and origin of each alarm when there are more than one against the same MO, see the Hardware Error Log Entries table for that MO.

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 1: Alarm reporting flowchart on page 30).

Figure 1: Alarm reporting flowchart



Alarm reporting options

Avaya's comprehensive maintenance design includes adjustable Communication Manager parameters to provide you with a suitable level of alarm-reporting information. Contact your Avaya representative to discuss how to set the **Alarm Reporting Options** form, because the **`set options`** command requires the *init* login level.

Be sure to set the alarm reporting parameters on the **Alarm Reporting Options** form so that they align with your Avaya maintenance contract. For example, you might want to downgrade Off-board TCP/IP Link Alarms so that they are not reported to the INADS group if you have tools or personnel to help monitor the LAN/WAN across the enterprise.

Figure 2 and Figure 3 are examples of the **Alarm Reporting Options** screens that show the many ways to configure Communication Manager for detailed maintenance information.

Figure 2: Set options form, page 1

```
set options                                                  Page   1 of  22
                            ALARM REPORTING OPTIONS

                                                    Major   Minor
                              On-board Station Alarms: w      w
                             Off-board Station Alarms: w      w
                 On-board Trunk Alarms (Alarm Group 1): y      y
                Off-board Trunk Alarms (Alarm Group 1): w      w
                 On-board Trunk Alarms (Alarm Group 2): m      w
                Off-board Trunk Alarms (Alarm Group 2): w      w
                 On-board Trunk Alarms (Alarm Group 3): r      w
                Off-board Trunk Alarms (Alarm Group 3): w      w
                 On-board Trunk Alarms (Alarm Group 4): n      w
                Off-board Trunk Alarms (Alarm Group 4): w      w
                          On-board Adjunct Link Alarms: w      w
                         Off-board Adjunct Link Alarms: w      w
                            Off-board MASI Link Alarms:        w
                                  Off-board DS1 Alarms: w      w

                           Off-board TCP/IP Link Alarms: w      w
                               Off-board Alarms (Other): w      w
                           Off-board ATM Network Alarms:        w
```

Figure 3: Set options form, page 2

```
set options                                                Page   2 of  22
                              ALARM REPORTING OPTIONS

                                                      Major   Minor
                    Off-board Firmware Download Alarms:       w
                      Off-board Signaling Group Alarms:       w
                                    Remote Max Alarms:        w
                Off-board CLAN TCP/IP Ping Test Alarms:       w
```

The first two pages of the form list alarm groups by function and whether or not the alarm originates on- or off-board. The Major and Minor columns can have any of the following values:

- **m**(in) - minor alarm (downgrades a major alarm to minor)
- **n**(o) - does not report the alarm in the Alarm Log
- **r**(eport) - reports the alarm in the Alarm Log
- **w**(arning) - downgrades a major or minor alarm to a warning alarm
- **y**(es) - reports the alarm in the Alarm Log

Note:

You cannot downgrade the major alarms for the following fields: **Off-board MASI Link Alarms**, **Off-board ATM Network Alarms**, **Off-board Firmware Download Alarms**, **Off-board Signaling Group Alarms**, and the **Remote Max Alarms**.

The remaining pages (3-22) of the **Alarm Reporting Options** form allow you to group trunk groups and administer a collective alarm reporting strategy. For example, the Figure 4 shows the first 100 trunk groups by number.

Figure 4: Trunk group alarm options page

```
set options                                                    Page   3 of  22

                          TRUNK GROUP ALARM OPTIONS

                                   (Alarm Group)


01: 1   11: 1   21: 1   31: 2   41: 2   51: 3   61: 3   71: 3   81: 4   91: 4
02: 1   12: 1   22: 1   32: 2   42: 2   52: 3   62: 3   72: 3   82: 4   92: 4
03: 1   13: 1   23: 1   33: 2   43: 2   53: 3   63: 3   73: 3   83: 4   93: 4
04: 1   14: 1   24: 1   34: 2   44: 2   54: 3   64: 3   74: 3   84: 4   94: 4
05: 1   15: 1   25: 1   35: 2   45: 2   55: 3   65: 3   75: 3   85: 4   95: 4
06: 1   16: 1   26: 2   36: 2   46: 2   56: 3   66: 3   76: 4   86: 4   96: 4
07: 1   17: 1   27: 2   37: 2   47: 2   57: 3   67: 3   77: 4   87: 4   97: 4
08: 1   18: 1   28: 2   38: 2   48: 2   58: 3   68: 3   78: 4   88: 4   98: 4
09: 1   19: 1   29: 2   39: 2   49: 2   59: 3   69: 3   79: 4   89: 4   99: 4
10: 1   20: 1   30: 2   40: 2   50: 2   60: 3   70: 3   80: 4   90: 4   100: 4
```

In this example trunk groups 1-100 report alarms to the Alarm Log in the following ways:

- Trunk groups 1-25 are assigned to Alarm Group 1: on-board alarms report as-is (major and minor--see the **On-board Trunk Alarms (Alarm Group 1)** field in Figure 2: Set options form, page 1 on page 31). Both major and minor off-board alarms are downgraded to the warning alarms.
- Trunk groups 26-50 are assigned to Alarm Group 2: major on-board alarms report as minor alarms, and minor alarms report as warning alarms (**On-board Trunk Alarms (Alarm Group 2)** field in Figure 2: Set options form, page 1 on page 31). Both major and minor off-board alarms are downgraded to warning alarms.
- Trunk groups 51-75 are assigned to Alarm Group 3: major on-board alarms report as-is to the Alarm Log, and minor alarms report as warning alarms (**On-board Trunk Alarms (Alarm Group 3)** field in Figure 2: Set options form, page 1 on page 31). Both major and minor off-board alarms are downgraded to warning alarms.
- Trunk groups 76-100 are assigned to Alarm Group 4: major on-board alarms are not reported to the Alarm Log, and minor alarms report as warning alarms (**On-board Trunk Alarms (Alarm Group 4)** field in Figure 2: Set options form, page 1 on page 31). Both major and minor off-board alarms are downgraded to warning alarms.

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.
- 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 35 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 5: Intra-port and Inter-port data transmission states on page 37 is a pictorial guide through intra-port and inter-port data transmission state changes that 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 5 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.

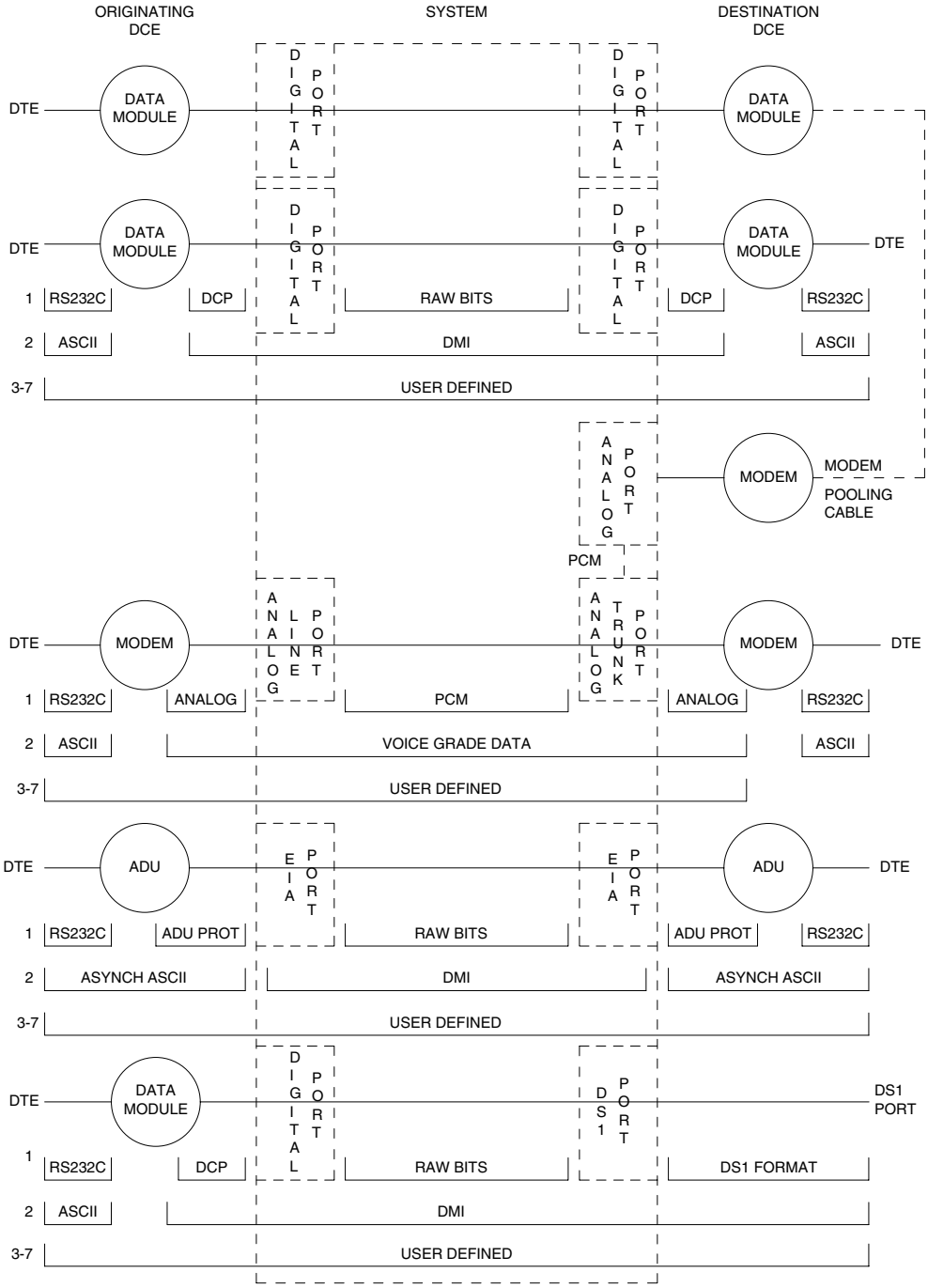
Therefore, for ISDN transmissions, BRI terminals and data modules, and DS1 ports insert, interpret, and strip both Layer-2 DCE information and Layer-3 elements. Also, the DS1 port passes Layer-3 elements to the system for processing. For more information about Layer 2 or 3, see OSI layers on page 36.

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 5: Intra-port and Inter-port data transmission states on page 37 as "user-defined," with no state changes until the transmission stream reaches its destination.

Figure 5: 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 5: Intra-port and Inter-port data transmission states on page 37.

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 summarizes the protocols used at various points in the data transmission stream. See also Figure 5: Intra-port and Inter-port data transmission states on page 37.

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 and Table 8.

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 5: Intra-port and Inter-port data transmission states on page 37 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 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 44 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 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 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 45 shows the overload and cross-talk.

Table 13: Overload and crosstalk

Overload level	+3 dBm0
Crosstalk loss	>70 dB

Intermodulation distortion

Table 14 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 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 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 shown in Table 17.

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 SFRL should meet or exceed 12 dB
Station to 4-wire trunk connection	ERL should meet or exceed 24 dB SFRL should meet or exceed 14 dB
Station to 2-wire trunk connection	ERL should meet or exceed 18 dB SFRL should meet or exceed 12 dB
4-wire to 4-wire trunk connection	ERL should meet or exceed 27 dB SFRL should meet or exceed 20 dB

Peak noise level

Table 18 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 48 through Table 21: MTS and WATS port circuit packs on page 49 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 and 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
TN790B 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 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 3: G700 MGP CLI Commands in *Maintenance Commands Reference (03-300431).*	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)

Removing and restoring EMBEDDED AUDIX power

Manually power down AUDIX System

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

Note:

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

1. Using a pointed object such as a paper clip or pen (do not use a pencil), press the **Boot/ Shutdown** button 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.

Manually power up AUDIX

To 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."

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/MM717)
- Analog Trunk/Telephone Port Media Module (MM711/MM714)
- T1/E1 Media Module (MM710)
- VoIP Media Module (MM760)
- BRI Media Module (MM720/MM722)

For procedures on adding, removing, or replacing Media Modules, refer to S8300 component maintenance on page 380.

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 S8300 component maintenance on page 380.

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 S8300 component maintenance on page 380.

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 S8300 connections on page 69.

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 3: G700 MGP CLI Commands in *Maintenance Commands Reference (03-300431)* 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 C360 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 55. 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 57 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 *1 of 6*

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 *2 of 6*

Media Module	Maintenance Object	Test	Executed for Media Module
BRI Trunk Media Module (MM720/ MM722) (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 *3 of 6*

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
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

3 of 6

Table 24: Media module tests *4 of 6*

Media Module	Maintenance Object	Test	Executed for Media Module
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
	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
			4 of 6

Table 24: Media module tests *5 of 6*

Media Module	Maintenance Object	Test	Executed for Media Module
	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 *6 of 6*

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 indicates why some tests are not executed on the G700.

Table 25: Tests not executed on the G700 platform *1 of 2*

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.

1 of 2

Table 25: Tests not executed on the G700 platform *2 of 2*

Test	Notes
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.
	2 of 2

Tone detector tests not executed on the G700

Table 26 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 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 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 specifies maintenance features as they apply to the Avaya G700 with the S8300 Media Server.

Table 29: Maintenance features for Avaya G700 Media Gateway *1 of 3*

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. This test aborts when attempting a test call on these trunk groups: • ISDN-PRI • SIP • DID • Any incoming trunk group (transmission tests can only be run on outgoing trunks)
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.

1 of 3

Table 29: Maintenance features for Avaya G700 Media Gateway *2 of 3*

Supported feature	Controller S8700/ S8500 S8300	Notes
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.
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: Archangel Network Control Element Packet Interface TDM clock Tone generator 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	

2 of 3

Table 29: Maintenance features for Avaya G700 Media Gateway *3 of 3*

Supported feature	Controller S8700/ S8500 S8300	Notes
Write Physical Angel command	No	
System synchronization	No	
		3 of 3

Chapter 2: Access and login procedures

This chapter describes the various ways of connecting to and logging into Avaya media servers and gateways.

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

This chapter contains information on these topics:

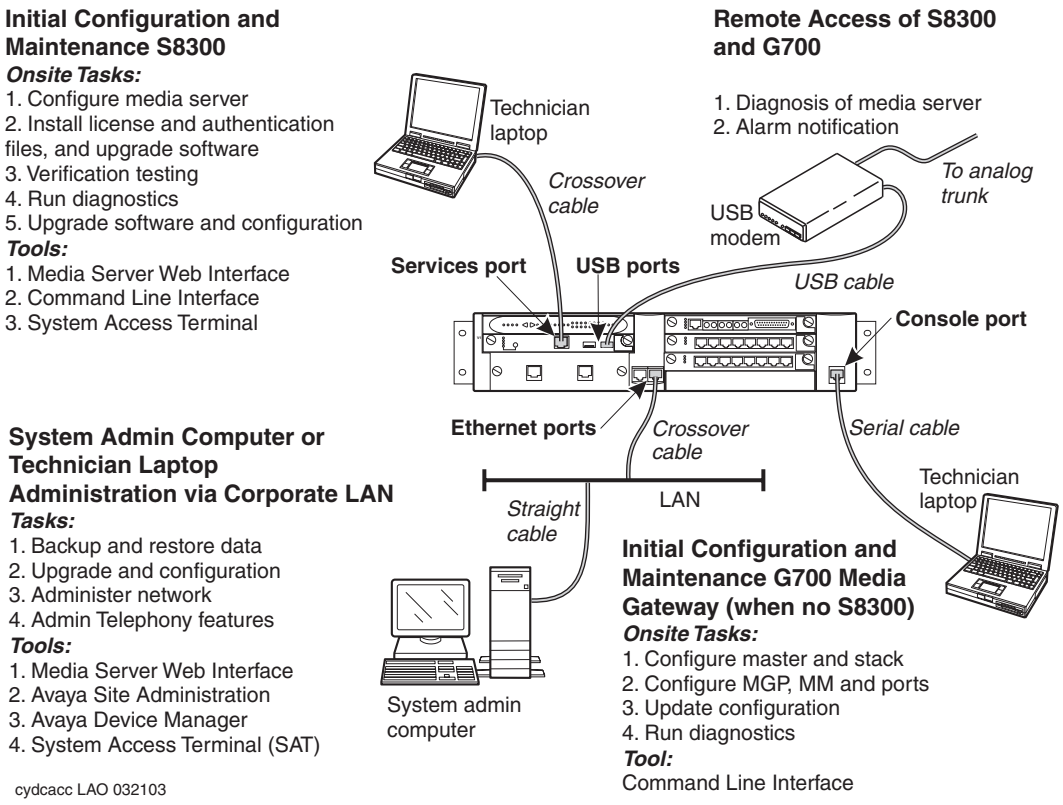
- S8300 connections
- Secure access
  - Secure Shell and Secure FTP
  - Secure Copy
- Login methods
- Navigating the Command Line Interface

S8300 connections

Review physical access methods

1. Check the Figure 6: Summary of S8300 and G700 access methods and tasks on page 70 for the location of the S8300 Services port.

Figure 6: 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

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 72
   - Windows 95, 98, NT 4.0, and ME: change TCP/IP properties on page 73

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:
   a. Click the radio button labeled **Use the following DNS server addresses**. The entries for **Preferred DNS server** and **Alternate DNS server** should both be blank.
   b. Click the **Advanced** button at the bottom of the screen. The **Advanced TCP/IP Settings** screen appears.
   c. Click the **DNS** tab and verify that no DNS server is administered (the **Address** field should be blank).
9. Disable WINS Resolution as follows:
   a. Click the **WINS** tab. Make sure WINS is not administered (the **Address** field should be blank).
   b. Click **OK**. If warned about an empty primary WINS address, click **Yes** to continue.
10. Click **OK** twice to accept the address information and close the **TCP/IP and Local Area Connection Properties** dialog boxes.
11. Reboot the system if directed to do so.

    After you have made these changes to your computer's network configuration information, the **Network and Dial-up Connections** window shows the status of the Local Area Connection:
    - Enabled appears when the laptop's Ethernet cable is connected to the server.
    - Disabled or unplugged appears if the NIC is not connected to anything.

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 semicolon (;).
     - 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 semicolon (;).
     - 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 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 C360 device in the stack as follows:
   - G700 Media Gateway: a lit MSTR LED indicates that this unit is the stack master.
   - A non-G700 C360 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 C360 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 91), 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 77.

   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 dropdown 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 91.

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 > Programs > Avaya > 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 dropdown 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 dropdown 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 dropdown 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. Type **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 91.

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 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 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

Secure access

If you are accessing the server with the URL "http://server-name," immediately you will be redirected to the secure URL "https://server-name" that uses port 443. When accessing a server URL, there is no need to have port 80 open.

This section also describes security-enhanced methods for remote access and copying through

- Secure Shell and Secure FTP
- Secure Copy

Following those discussions is the Administration section that describes how to disable Telnet and FTP/TFTP.

Secure Shell and Secure FTP

The Secure Shell (SSH) and Secure FTP (SFTP) capabilities are highly-secure methods for remote access. Administration for this capability also allows a system administrator to disable Telnet when it is not needed, making for a more secure system.

SSH/SFTP functionality does not require a separate Avaya license, nor are there any entries in the existing Communication Manager license needed.

Topics in this section include:

- Applicable platforms or hardware
- Symmetric algorithms
- Secure access comparisons
- Host keys

Applicable platforms or hardware

You can log in remotely to the following platforms or hardware using SSH as a secure protocol:

- G350 Media Gateway
- C350 Multilayer Modular switch
- S8300, S8500, S8700, or S8710 Media Server command line
- IBM eserver BladeCenter Type 8677 command line
- Communication Manager System Administration Terminal (SAT) interface on a media server using port 5022.

Note:

The client device for remote login must also be enabled and configured for SSH. Refer to your client PC documentation for instructions on the proper commands for SSH.

Secure Shell (SSH) and/or Secure FTP (SFTP) remote access protocols are provided on these circuit packs:

- TN799DP (CLAN)
- TN2501AP (VAL)
- TN2312AP/BP (IPSI)
- TN2602AP (Crossfire)

SAT commands enable S/FTP sessions through login/password authentication on the CLAN and VAL circuit packs and SSH/Telnet on the Crossfire circuit pack. The Maintenance Web Interface and a Communication Manager command line enable the IPSI session. Unencrypted Telnet and FTP capabilities are enabled on these circuit packs.

Symmetric algorithms

SAT commands enable the CLAN, VAL, IPSI, and Crossfire circuit packs as SSH/SFTP servers that prefer the following symmetric algorithms in decreasing order:

- AES
- Arfour
- Blowfish
- CAST128
- 3DES

Note:

These are the only algorithms supported. To ensure that technicians can access the relevant circuit packs using SSH or SFTP, technician laptops must have SSH and SFTP clients that use at least one of the above algorithms installed.

Secure access comparisons

Table 33 summarizes the hardware, software, Communication Manager releases, commands, and protocols.

Table 33: Comparison of SSH/SFTP capabilities

Circuit pack	Release 3.0		Release 3.1	
	Command[1]	**Result**	**Command**[2]	**Result**
TN799DP (CLAN)	**enable/disable filexfr**	Enables/disables S/FTP	**enable/disable filexfr**	Enables/disables S/FTP
TN2501AP (VAL)	**enable/disable filexfr**	Enables/disables S/FTP	**enable/disable filexfr**	Enables/disables S/FTP
TN2312AP/BP (IPSI)	**ipsisession loadipsi**	Enables SSH/Telnet[3] Enables SFTP[4]	**ipsisession loadipsi**	Enables SSH/Telnet[3] Enables SFTP[4]
TN2602AP Crossfire	**enable session (Secure? = n)**	Enables Telnet (not SSH)	**enable/disable filexfer enable/disable session**[5]	Enables/disables S/FTP Enables/disables SSH

1. Issue commands for CLAN and VAL from the SAT; issue the **ipsisession** from the IPSI command line interface (CLI).
2. Issue commands for CLAN and VAL from the SAT; issue the **ipsisession** from the IPSI command line interface (CLI).
3. The **ipsisession** command enables Telnet on IPSI circuit packs that do not support SSH.
4. The **loadipsi** command enables FTP on circuit packs that do not support SFTP.
5. When moving from secure to insecure sessions or vice-versa, you must disable the established session before attempting the next.

Note:

Telnet can also be used if enabled by the customer on the server, but it is inherently a less secure connection.

Host keys

Public key exchange - TN circuit packs support dynamic host keys, and since clients have the server's public key information stored on them, when the server generates a new public/private key pair (which happens the first time the board initializes or when the user decides), the client prompts the user to accept the key when logging into the server. This is to make the client user aware that the server's public key is not what it used to be and this may, but not necessarily, imply a rogue server. A technician encountering this situation should determine if the server's keys were changed since the last servicing.

- If they were, the technician should continue login.
- If not, there is a security issue, and the technician should notify the appropriate personnel.

Resetting the dynamic host keys - You can reset the dynamic host keys on any of the supported circuit packs by executing a command either from the SAT or the command line interface (CLI), as detailed in Table 34.

Note:

You must busyout the circuit pack (**busyout board *location***) before issuing the command to reset the dynamic host keys.

Table 34: Reset dynamic host keys commands

Circuit pack	Command issued from	Command	Permissions
TN799DP (CLAN)	SAT	**reset ssh-keys board *location***	*craft/dadmin* or higher
TN2501AP (VAL)	SAT	**reset ssh-keys board *location***	*craft/dadmin* or higher
TN2312AP/BP (IPSI)	CLI	**ssh-keygen**	*craft/dadmin* or higher
TN2602AP (Crossfire)	SAT	**reset ssh-keys board *location***	*craft/dadmin* or higher

See *Maintenance Commands Reference (03-300431)* for additional information about these commands.

Enabling and disabling secure sessions on circuit packs

This procedure applies only to these circuit packs and software version:

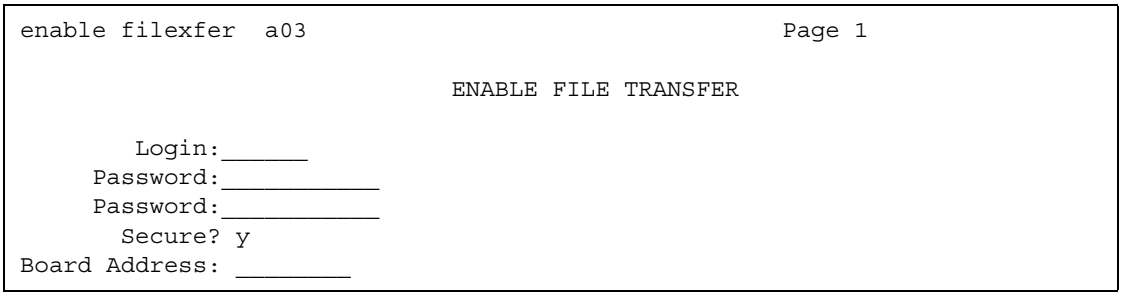
- TN799DP (CLAN) with Release 3.0 firmware or higher
- TN2501AP (VAL) with Release 3.0 firmware or higher
- lTN2602AP (Crossfire) with Release 3.1 firmware or higher
- Communication Manager, Release 3.0 or higher

To enable an S/FTP session on a CLAN or VAL circuit pack:

1. At the SAT type **enable filexfr** and press **Enter**.

   The **Enable File Transfer** screen displays.

Figure 7: Enable File Transfer screen



2. Type a 3-6 alphabetic character login in the **Login** field.
3. Type a 7-11 character password (at least one letter and one number) in the first **Password** field.
4. Retype the same password in the second **Password** field.
5. Type **y** in the **Secure?** field to enable SFTP; type **n** for FTP.
6. Submit the form.

   S/FTP is enabled on the circuit pack, and the login/password are valid until you disable the session.

To disable an S/FTP session on a CLAN or VAL circuit pack:

1. At the SAT type **`disable filexfr board`** ***`location`*** and press **Enter**.

   S/FTP is disabled on the circuit pack.

Enabling and disabling secure sessions on Crossfire

This procedure applies only to TN2602AP (Crossfire) circuit packs.

To enable an S/FTP session on a Crossfire circuit pack:

1. At the SAT type **`enable session`** and press **Enter**.

   The **Enable Session** screen displays.

Figure 8: Enable Session screen

```
enable session                                              Page   1 of   1


                                  ENABLE SESSION

                    Login:
                 Password:
          Reenter Password:
                   Secure?
             Time to login:
             Board address:
```

2. Type a 3-6 alphabetic character login in the **Login** field.
3. Type a 7-11 character password (at least one letter and one number) in the first **Password** field.
4. Retype the same password in the second **Password** field.
5. Type **y** in the **Secure?** field to enable SFTP; type **n** for FTP.
6. The **Time to login** field requires numerical entries in minutes with a range of 0 – 255.
7. Type the location in the **Board address** field.
8. Submit the form.

   S/FTP is enabled on the circuit pack, and the login/password are valid until you disable the session.

To disable an S/FTP session on a Crossfire circuit pack:

1. At the SAT type **`disable session board`** ***`location`*** and press **Enter**.

   S/FTP is disabled on the circuit pack.

Secure Copy

You can transfer files to and from the G350 Media Gateway, the TN799DP CLAN circuit pack, and the C360 Multilayer Modular switch using Secure Copy (SCP). The primary purpose of SCP for these devices is downloading firmware. The SCP capability allows a system administrator to disable File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) when they are not needed, making for a more secure system.

This feature is supported on the following devices:

- S8300 Media Server
- S8500 Media Server
- S8700 Media Server

- G350 Media Gateway
- TN799DP CLAN circuit pack
- C360 Multilayer Modular switch

Note:

The target device for SCP data transfer must also be enabled for SCP. Refer to your client PC documentation for instructions on the proper commands for SCP.

Interactions

You can use SCP

- To download firmware to the various media modules on the G350 Media Gateway.
- With FTP enabled or disabled.
- With TFTP enabled or disabled.

Administration

Turning off Telnet for increased security

If you are using SSH to log in to the server or gateway, you might want to turn off Telnet for an extra level of security. To turn off Telnet, do the following:

1. On the Maintenance Web page main menu, click on **Firewall**.

   The system displays the Firewall page.
2. Click the **Telnet Input to Server** boxes so that the check mark disappears.
3. Click the **Telnet Output from Server** box so that the check mark disappears.
4. Click the **Submit** button.

Turning off FTP and TFTP for increased security

If you are using SCP to copy files to the server or G350 Media Gateway, you may wish to turn off FTP or TFTP for an extra level of security. To turn off these features, do the following:

1. On the Maintenance Web page main menu, click on **Firewall**.

   The system displays the Firewall page.
2. Click the **FTP or TFTP Input to Server** boxes so that the check mark disappears.
3. Click the **FTP or TFTP Output from Server** box so that the check mark disappears.
4. Click the **Submit** button.

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 **Start > Run**.
   - Type **`telnet 192.11.13.6`** to access the media server CLI.
3. When the login prompt appears, log in to the server with the appropriate user name and password.
4. 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**.
5. 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 displays.
3. Click the **Continue** button.
4. Accept the server security certificate.

   The **Login** screen displays.
5. Log in as *craft*.

   The main menu displays.
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.
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 C360 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 (**telnet 192.11.13.6**).
2. Login as *craft* or *cust*.
3. Telnet to the Layer 2 stack master processor.

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

4. Login at the Welcome to Avaya C360 screen.
   - Login: from the planning documentation
   - Password: from the planning documentation

   You are now logged-in at the Supervisor level. The prompt appears as *C360-1(super)#*.

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 C360 stack processor IP address (**`telnet ip-address`**, where ***`ip-address`*** is the IP address of the C360 stack master processor on the customer's LAN).
2. Login at the Welcome to Avaya C360 screen.
   - Login: from the planning documentation
   - Password: from the planning documentation

   You are now logged-in at the Supervisor level. The prompt appears as *C360-1(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 HyperTerminal or any other terminal emulation program (**Start > Programs > Accessories**).
2. Choose **Call - Connect** (for HyperTerminal) or the appropriate call command for your terminal emulation program.
3. Login at the Welcome to Avaya C360 screen.
   - Login: from the planning documentation
   - Password: from the planning documentation

   You are now logged-in at the Supervisor level. The prompt appears as *C360-1(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://C360-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.

Navigating the Command Line Interface

Table 35 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 C360-1(super)# command-line prompt.

Table 35: Navigational aid for CLI commands *1 of 2*

Command	Purpose	Prompt
super	Change to supervisor mode	C360-1(super)# or <MG name>-1(super)#
configure	Change to configuration mode	C360-1(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	C360-1(super)#
session icc (from an MGP session)	Open a CLI session on the S8300 processor	craft@<host name>>
session *session#*	Open a session on the stack processor in module in the stack	C360-<#>(super)#

1 of 2

Table 35: Navigational aid for CLI commands *2 of 2*

Command	Purpose	Prompt
exit	Close the current session and revert to the previous session	
command **help**	Displays help for ***command***	
		2 of 2

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.

Chapter 3: S8400 Maintenance Processor Complex

S8400

The Avaya Maintenance Processor Complex (MPC) functionality is co-resident on the Avaya S8400 Media Server (TN8400AP). The MPC features include:

- Monitors the health of the server hardware including temperature
- Reports server hardware failure and other alarms to INADS by modem
- Remote server soft and hard resets
- Remote access dial-in connection to the server
- Local laptop access to the server

Access to the MPC is through a browser or through the command line. You can use any Web browser that supports cascading style sheets and Javascript to remotely access the MPC:

Note:

The examples and/or values in all windows shown are examples. Your settings might be different.

Topics in this section include:

- Login administration on page 97
- Connecting and logging in to the MPC on page 99
- MPC Web interface on page 104
- Verifying the internal link on page 118
- Disabling the boot timer on page 118
- Password protection on page 120
- Updating the MPC firmware on page 121

Login administration

Topics in this section include:

- Creating a remote (modem) login on page 98
- Creating a local (MPC) login on page 98
- Changing a local login to a remote login on page 99
- Changing a remote login to a local login on page 99
- Removing a MPC login on page 99

Creating a remote (modem) login

To create a remote login for use over a modem:

1. On the host, type **rmbuseradd -P y *login*** and press **Enter**, where ***login*** is the unique login name. The login:
   - can have upper or lower case letters
   - cannot exceed 12 characters
   - first character cannot be a number
2. Type **rmbpasswd *login*** and press **Enter**, where ***login*** is the unique login name.

   The system responds with `Enter password`.
3. Type the new password and press **Enter**.

   The system responds with `Re-enter the password`.
4. Type the new password again and press **Enter**.

Creating a local (MPC) login

To create a local login for use on the MPC:

1. On the host, type **rmbuseradd *login*** and press **Enter**, where ***login*** is the unique login name.
2. Type **rmbpasswd *login*** and press **Enter**, where ***login*** is the unique login name.The login:
   - can have upper or lower case letters
   - cannot exceed 12 characters
   - first character cannot be a number

   The system responds with `Enter password`.
3. Type the new password and press **Enter**.

   The system responds with `Re-enter the password`.
4. Type the new password and press **Enter**.

Changing a local login to a remote login

To change a local login to a remote login:

1. On the host, type **rmbusermod -P y *login*** and press **Enter** where ***login*** is the unique login name.

Changing a remote login to a local login

To change a remote login to a local login:

1. On the host, type **rmbusermod -P n *login*** and press **Enter**, where ***login*** is the unique login name.

Removing a MPC login

To remove a MPC login:

1. On the host, type **rmbuserdel *login*** and press **Enter**, where ***login*** is the unique login name.

Connecting and logging in to the MPC

Note:

To access the MPC using SSH or the MPC Web interface, you must log into the MPC.

This section contains these topics:

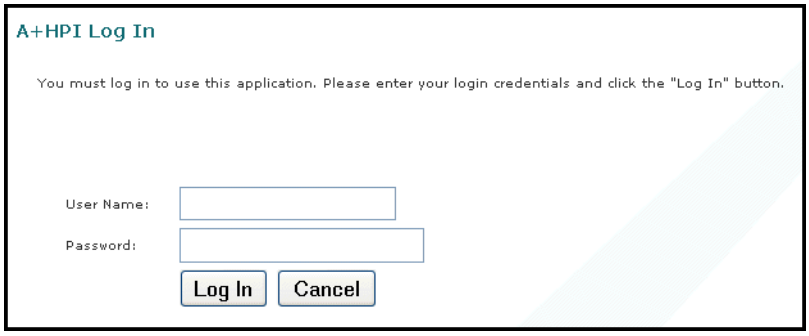
- Connecting through a Web browser on page 99
- Connecting locally through SSH on page 101
- Connecting remotely through SSH on page 101

Connecting through a Web browser

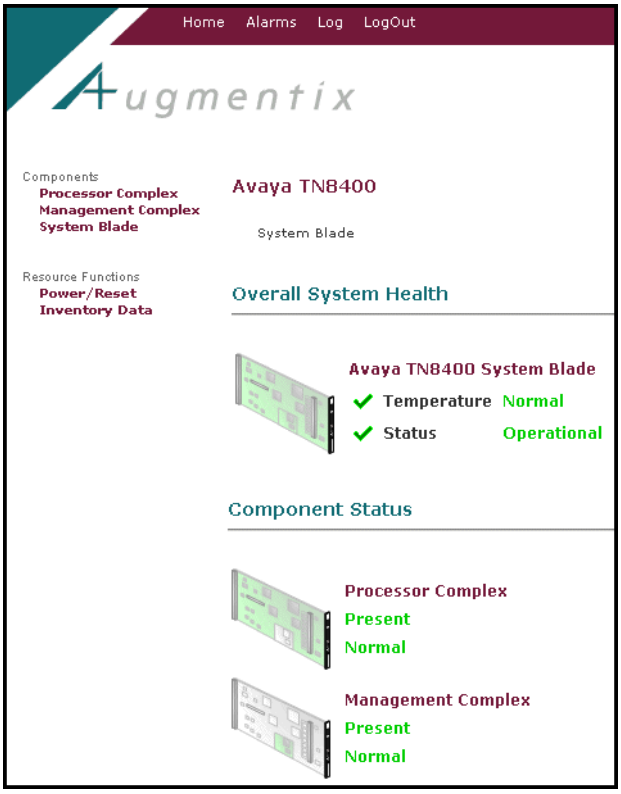
To connect to the MPC through a Web browser:

1. Connect the services laptop to the front panel using a crossover cable.

2. Open Web browser window.
3. In the **Address** field, type `https://192.11.13.6:10443` and press **Enter**.
   The system displays the **Log In** window.



4. In the **User Name** field, type **craft**.
5. Type the appropriate password in the **Password** field and click on the **Log In** button.
   The system displays the **Home** window.



Connecting locally through SSH

To connect to the MPC using the Secure Shell (SSH) protocol through a secure client like PuTTy:

1. On the Services laptop, select **Start** > **Programs** > **PuTTY** > **PuTTY**.

   The system displays the **PuTTY Configuration** window

2. In the **Host Name (or IP address)** field, type **192.11.13.6**.

3. In the **Port** field, type **10022**.

   This port might be different with Avaya's other products that use SSH. If you plan to connect to the server, then use port 22.

4. Click **Open**.

   The system displays the **PuTTY Security Alert** window the first time you contact to a MPC with this version of PuTTY.

5. Click **Yes** to accept the server's host key.

   The system displays the **PuTTY** window.

6. Log in as **craft**.

   The system prompt displays.

7. To disconnect type **exit** and press **Enter**.

Connecting remotely through SSH

Note:

Remote connections work the same as if the modem was connected to the server.

To connect to the MPC using a remote SSH connection:

1. On a command line interface (CLI), type **connect2 -p *modem telephone number* -l *login* -c *login password* -t *product type* -R *RAS access password*** and press **Enter**.

   The system dials into the modem, establishes a PPP connection and displays (example):

   Open another window on this machine, and connect the desired tool to Address 10.7.9.2

   When you are finished with your connection, come back to this window, and press Enter to manually shut it down.

2. Open another CLI window.

3. Type **ssh -p 10022 craft@*address provided above*** and press **Enter**.

   For example, **ssh -p 10022 craft@10.7.9.2**.

4. In the password, type the server password for **craft** and press **Enter**.

   The system prompt displays.

5. When done, type **exit** and press **Enter**.

6. Go back to the first window and press **Enter** to close it.

Connecting remotely through a Web browser

To remotely connect to the MPC using a Web browser:

1. On a command line interface (CLI), type **connect2 -p *modem telephone number* -l *login* -c *login password* -t *product type* -R *RAS access password*** and press **Enter**.

   The system dials into the modem and establishes a PPP connection.

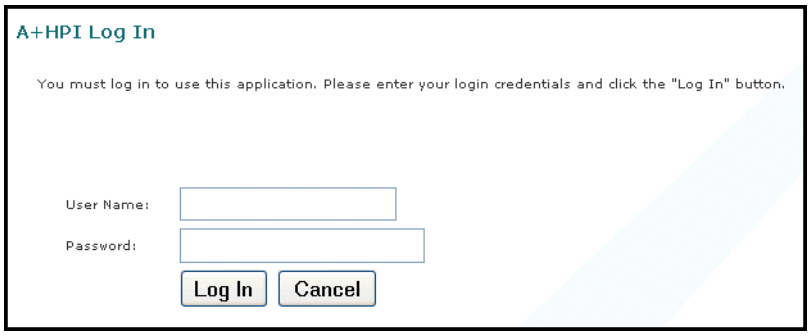
   The system responds with:

   ```
   Open another window on this machine, and connect the desired tool to
              Address 10.7.9.2
   When you are finished with your connection, come back to this window, and
   press Enter to manually shut it down.
   ```

2. Open a Web browser window.

3. In the **Address** field, type **https://10.7.9.2:10443** and press **Enter**.

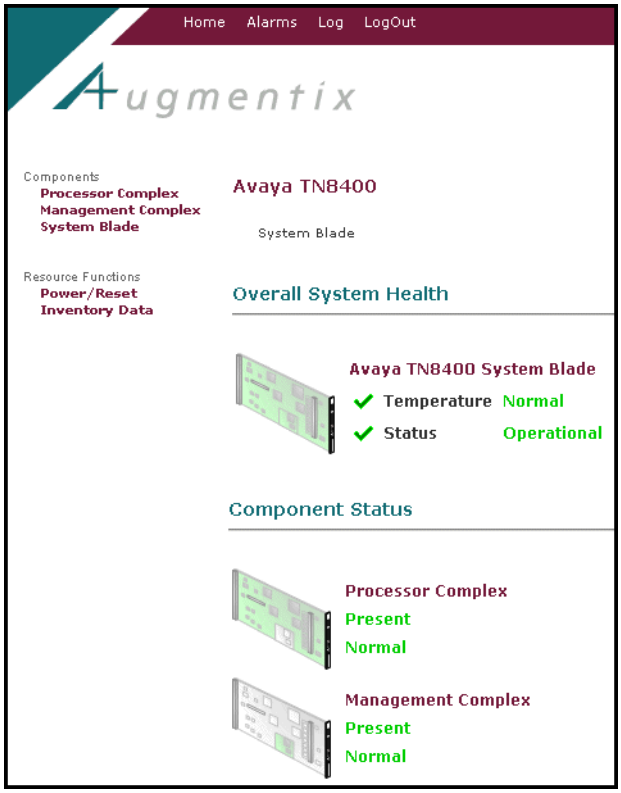
   The system displays the **Log In** window.



4. In the **User Name** field, type **craft**.

5. In the **Password** field, type the server password for **craft** and click **Log In**.

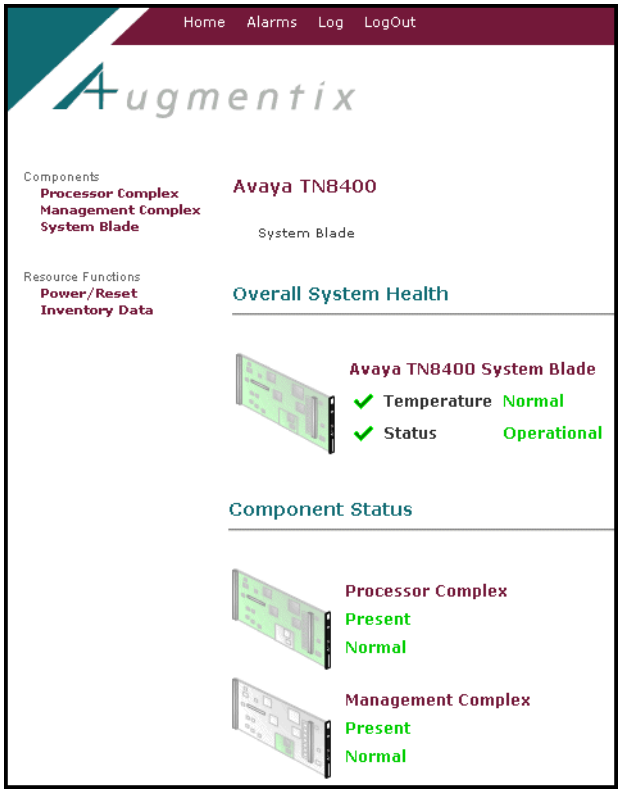
   The system displays the **Home** window.



MPC Web interface

Home page

The **Home** page has basic links at the top, a navigation pane on the left, and a display pane in the middle of the page.



Note:

The MPC Web pages do not refresh automatically. To refresh the page use the Refresh functionality of your Web browser.

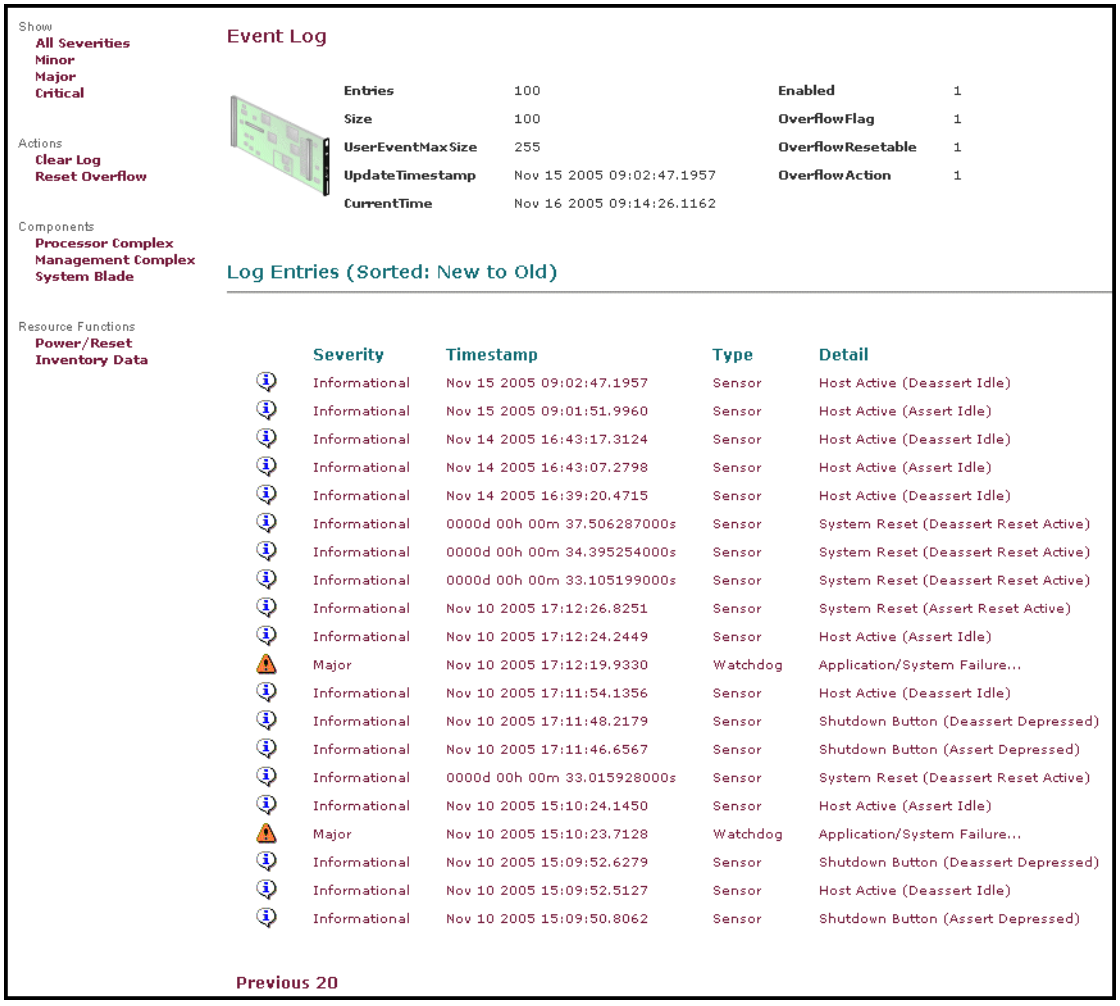
Table 36 lists the functions on the MPC Home page.

Table 36: MPC Home page

Function	Description
Home	Home window
Alarms	Shows information on the current active alarms
Log	Shows information on the last 100 events
Log Out	Terminates the MPC session
Components	
Processor Complex	Displays current conditions for the blade processor (not the Communication Manager processor)
Management Complex	Displays current MPC alarm, modem, and USB conditions
System Blade / Overall System Health	Displays the general system health of the Avaya S8400 Media Server
Resource Functions	
Power / Reset	Provides the remote power on, power cycle, and reset (soft and hard) capability on the server.
Inventory Data	Shows the server / manufacturer data
System Blade / Overall System Health	
Temperature	Shows the server and processor temperatures
Status	Shows the overall server status
Component Status	
Processor Complex	Displays current conditions for the blade processor (not the Communication Manager processor)
Management Complex	Displays current MPC alarm, modem, and USB conditions

Log

The **Event Log** page displays up to 100 events (twenty per page) in the MPC log beginning with the most recent event.



The Show section (upper-left corner of the page) can filter the log report on these parameters:

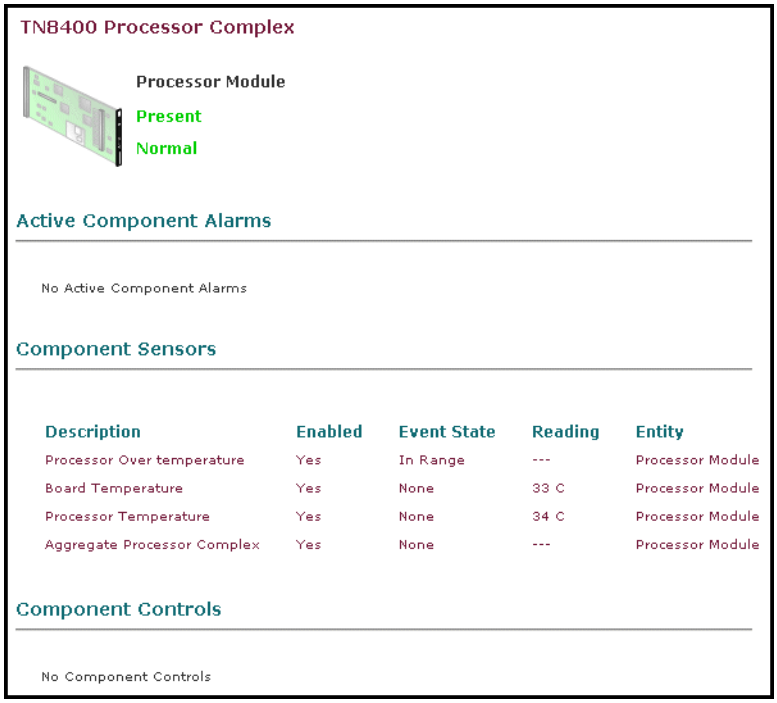
- **All Severities** displays all event levels.
- **Minor** displays only the minor events.
- **Major** displays only the major events.
- **Critical** displays only the critical events.

The **Action** section includes these activities:

- **Clear Log** removes all MPC log entries.
- **Reset Overflow** removes all overflow log entries and resets the overflow accumulation.

Processor Complex

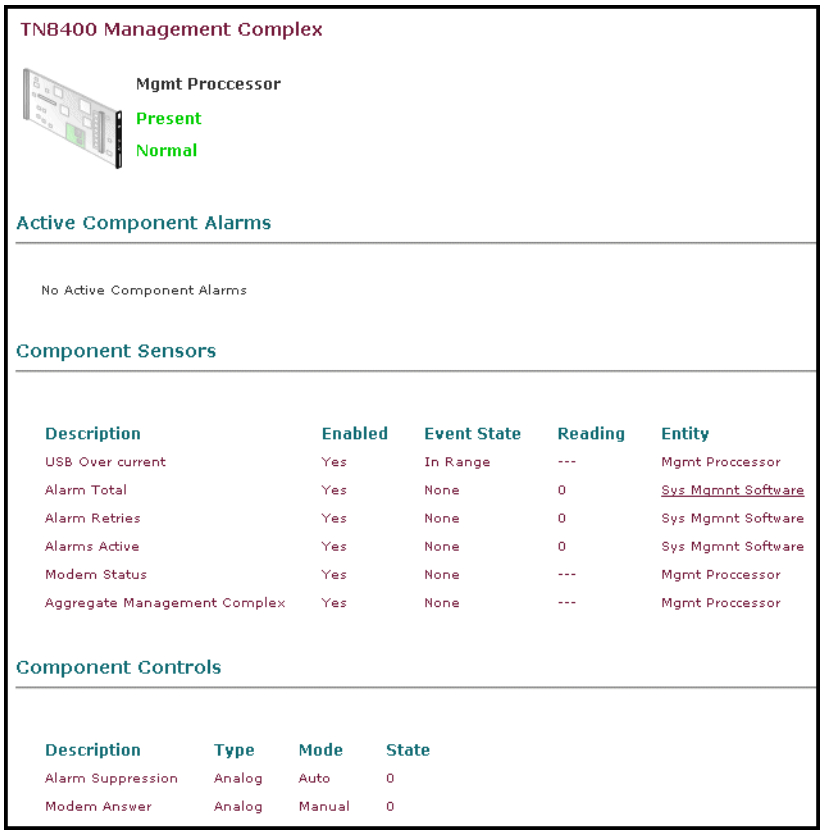
The **TN8400 Processor Complex** page displays current conditions for the MPC processor.



Component	Description
Processor Over Temperature	"In Range" indicates that the temperature is within the prescribed range.
Board Temperature	Temperature of the TN8400 server circuit pack
Processor Temperature	Temperature of the processor chip on the TN8400 server circuit pack
Aggregate Processor Complex	The aggregate status of the processor complex (not the Communication Manager processor) and a summation of the overall health

Management Complex

The **TN8400 Management Complex** page displays current alarm, modem, and USB conditions for the MPC.



- The **Enable** column indicates whether the sensor is enabled or not.

- The **Event State** column indicates which event state is active. In the case of an over current sensor, the event state of **In Range** indicates that an over current condition does not exist.
- Sensors typically have an event state and/or a reading. These columns indicate the current state and value of the sensor. If the sensor reading is "---", then the sensor does not support a reading, Sensors that do not support a reading indicate their state through the **Event State** column.

Component	Description
Component Sensors	
USB Over current	The sensor for the USB modem
Alarm Total	The **Reading** column displays the total number of alarms.
Alarm Retries	The number of alarms that were resent.
Alarms Active	The **Reading** column displays the number of active alarms.
Modem Status	The **Event State** indicates the current state of the modem status sensor: ● When the modem is not active, the status is **None**. ● When an outbound call is active, the event state is **Dial-Out Active**. ● Wand when an inbound call is active, the event state is **Dial-In Active**.
Aggregate Management Complex	The overall summary (aggregate) status of the MPC

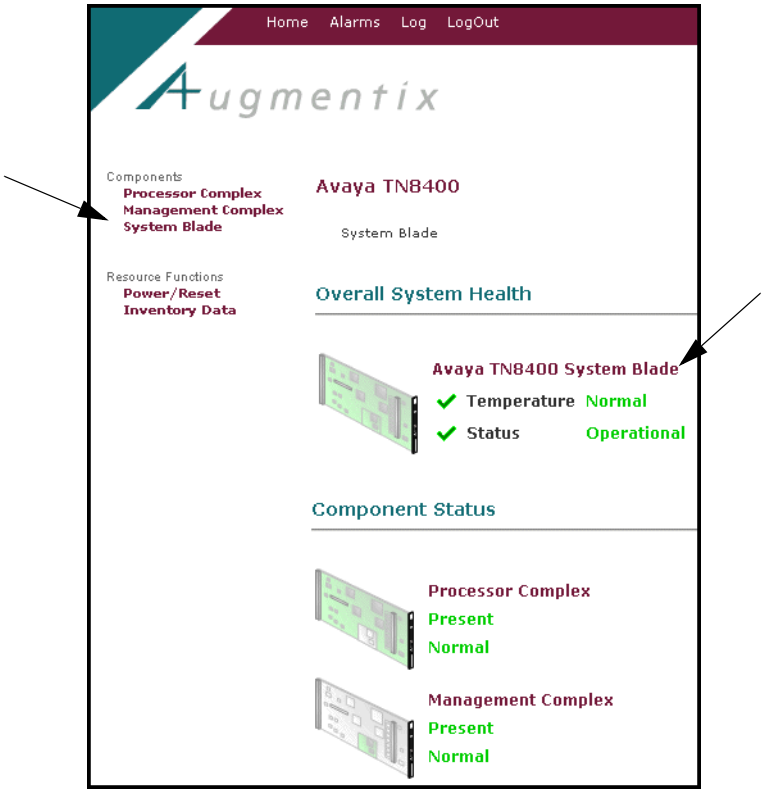
1 of 2

Component	Description
Component Controls	
Alarm Suppression	For all controls, the **Type** column indicates the value type for the control. A type of **Analog** means that you can set the Alarm Suppression control in minutes, for example: ● Setting the control to **30**, means that alarms will be suppressed for 30 minutes. ● Setting the control value to **20** means that alarms will be suppressed for 20 minutes ● Setting a value of **0** means that alarms will not be suppressed.
Modem Answer	The **Type**, **Mode**, and **State** columns interact according to these examples: ● The **Type** column indicates the modem type, in this example, **Analog**. ● When the **Mode** is set to **Auto**, the modem answers all incoming calls. ● When the **Mode** is set to **Manual**, the modem only answers *n* number of calls, where *n* is the **State** value. - If the **Mode** is **Manual** and the **State** value is **0**, then the modem will not answer any calls. - If the **Mode** is **Manual** and the **State** value is **1**, then the modem will answer 1 call.
	2 of 2

System Blade / Overall System Health

To view the general system health of the Avaya S8400 Media Server:

1. Select either **System Blade** (see arrow) in the Components section of the left navigation pane or **Avaya TN8400 System Blade** (see arrow) in the Overall System Health section of the **Home** page.



The **Avaya TN8400 Blade Server** page displays.

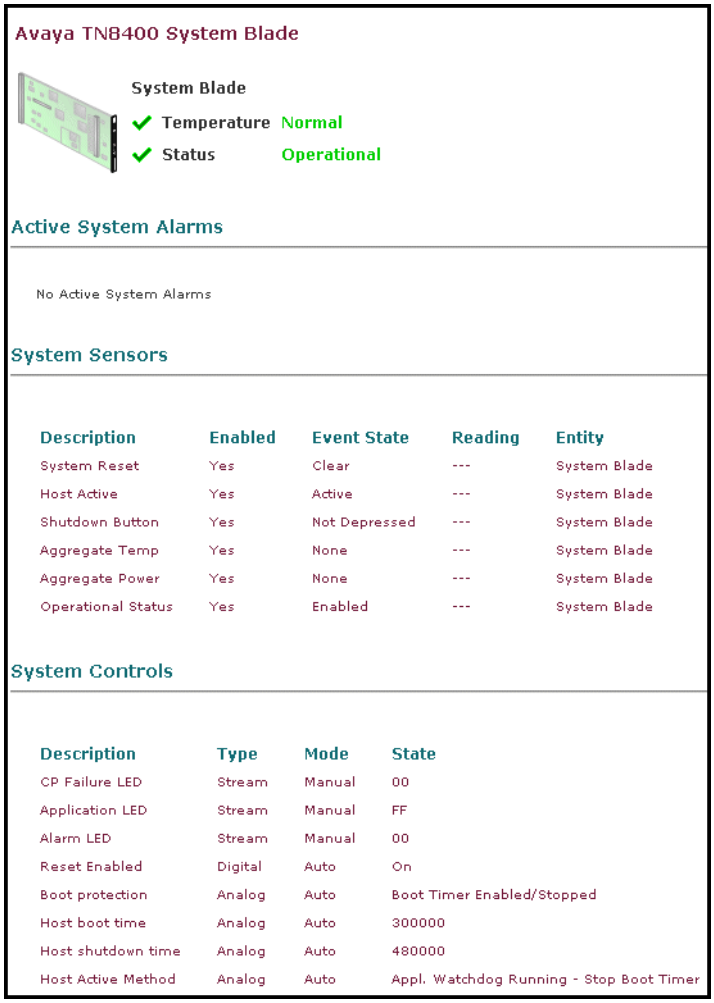


Table 37 describes the information on the Overall System Health page.

Table 37: MPC-Overall System Health page *1 of 2*

Field	Description
System Blade	
Temperature	Lists the temperature of the TN8400
Status	Overall health of the TN8400
System Sensors	
System Reset	The **Event State** indicates the current status of System Reset: • **Clear** indicates that reset is not asserted. • **Reset Active** indicates that reset is currently asserted.
Host Active	Indicates whether the server is up
Shutdown Button	Indicates whether the front-panel shutdown button is depressed or not.
Aggregate Temp	The **Event State** indicates the summary state of power on the server: • **None** indicates that system power is good. • Other possible event states include **Minor**, **Major**, and **Critical**.
Aggregate Power	The **Event State** indicates the summary state of power on the server: • **None** indicates that system power is good. • Other possible event states include **Minor**, **Major**, and **Critical**.
Operational Status	The **Event State** indicates the operational status of the circuit pack: • **Disabled** means the circuit pack is not operational (no heartbeat). • **Enabled** means the circuit pack is operational.
System Controls	
CP Failure LED	These controls indicate the current state of the specified front panel LED and allow a user to set the state of the LED by setting the control value.
Application LED	
Alarm LED	
Reset Enabled	Enables or disables reset control

1 of 2

Table 37: MPC-Overall System Health page *2 of 2*

Field	Description
Boot Protection	MPC monitors when the server boots up. See Disabling the boot timer through the Web interface on page 118 or Disabling the boot timeout using Linux commands on page 119.
Host Boot Timer	Sets the time allowed (in milliseconds) for a system to boot before the boot protection timer expires (default is 300,000)
Host Shutdown Time	Sets the time (in milliseconds) for a system to shutdown before the host shutdown timer expires (default is 480,000)
Host Active Method	Sets the method the MPC uses to determine if the host is active (default is "Appl. Watchdog Running - Stop Boot Timer")
	2 of 2

In the **System Controls** section **Type** can be:

- **Analog** - can be set to a particular value
- **Digital** - turns on and off
- **Stream** - sets each individual bit

Mode describes the type of operation:

- **Auto** - standard
- **Manual** - overrides set values

Power / Reset

The **Power/Reset Control** page allows you to turn the power on, off, or restart the server.

Table 38 outlines the information that is available on **Power / Reset Control** window.

Table 38: Power/Reset Control window selections *1 of 2*

Function	Description
Power / Reset Control	
Server	Indicates whether the server is operational or not
Boot Control	Indicates whether the boot control is enabled or not
Reset / Shutdown Actions	
Warm Reset	Methodically terminates all processes and restarts the operating system.
Graceful Shutdown	Methodically terminates all processes and shuts the system down.

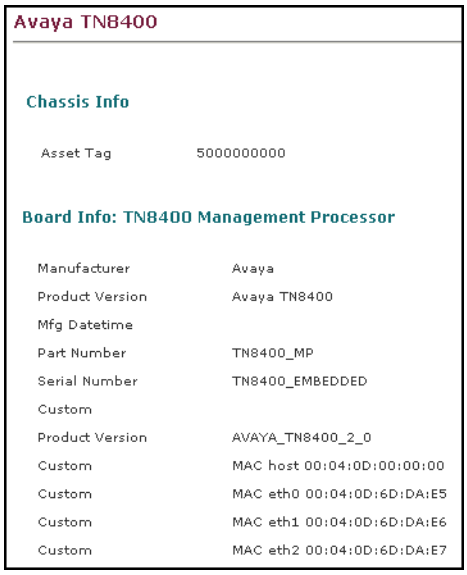
1 of 2

Table 38: Power/Reset Control window selections *2 of 2*

Function	Description
Cold Reset	Tells the server hardware to perform a "not so graceful" shutdown and restarts the operating system.
Boot Timer Actions	
Disable Boot Timer	Click on the Request Boot Timer Action to disable the operating system watchdog.
Enable Boot Timer	Reverses the effects of **Disable Boot Timer**. Normally, this should be enabled. When disabled, the MPC does not watch for the server to boot.
Refresh	Provides an updated screen. The screen may change depending on what has taken place in the last few minutes.
	2 of 2

Inventory Data

The **Inventory Data** page shows the server / manufacturer data.



Component	Description
Chassis Info	
Asset Tag	The Product ID set by the **`productid`** utility.
Board Info TN8400 Management Processor	
Manufacturer	
Product Version	The Product Version of the circuit pack
Mfg Datetime	Manufacturing date/time of the circuit pack
Part Number	Part or model number of the circuit pack
Serial Number	Serial number of the circuit pack that is set during manufacturing
Custom	Avaya Comcode that is set during manufacturing.
Product Version	Software image version on the MPC
Custom	Not applicable: MAC address of server (host)
Custom	MAC address of Ethernet port 0
Custom	MAC address of Ethernet port 1
Custom	MAC address of Ethernet port 2

Verifying the internal link

It is possible to verify the address of the MPC by pinging the suspected address. However, if that address is not the same as what the internal Ethernet port is configured as, the ping will fail. For example, if the internal Ethernet of the server is configured as 192.11.13.1 and the MPC is configured as 10.221.248.1, the command fails because the server and MPC are not on the same network. Consequently, the server network software will not attempt to send the ping down the internal interface.

To verify the internal link between the MPC and the server, perform the following steps:

1. Open a Telnet or SSH session to the server.
2. Log in as **craft**.
3. Type **`sampdiag -v`** and press **Enter**.
4. Look at the system response to determine if the MPC is communicating properly.

Disabling the boot timer

Although one of the MPC boot timer's primary functions is to monitor the reboot/boot, you should disable this function whenever you are replacing the solid state drive (SSD) on the S8400 server. Disabling the boot timer greatly increases the remastering reliability and decreases the time required.

Choose a method to disable the boot timer:

- Disabling the boot timer through the Web interface on page 118
- Disabling the boot timeout using Linux commands on page 119

Disabling the boot timer through the Web interface

To disable the boot timer through the MPC Web interface:

1. Connect the services laptop computer to the Services Port on the front panel of the S8400 server.
2. From a command window, type **`arp -d 192.11.13.6`**. Press **Enter**.
3. Open a browser window and type **https://192.11.13.6:10443** in the **Address** field.

   Note:

   This is the address for the MPC Web pages, not the Communication Manager Web pages. Also ensure that the URL is **https**.

   The MPC **Log In** page displays.

4. Log in as **craft**.

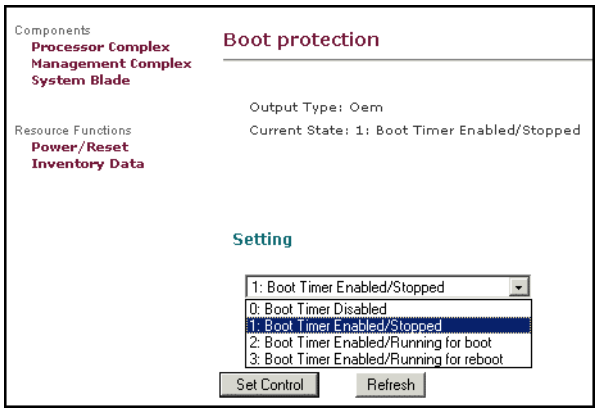
   The **Avaya TN8400 Home** page displays.

5. At the **Avaya TN8400 Home** window select the **System Blade** link.

   The System Blade / Overall System Health page displays.

6. In the System Controls section at the bottom of the page, click on the **Boot Protection** field or on the **Boot Timer Enabled/Stopped** link.

   The **Boot protection** page displays.



7. In the **Setting** field click on the pull-down menu and select **0: Boot timer Disabled** and then click on the **Set Control** button.

   After the remastering process is completed, Communication Manager reboots and sends the MPC a new set of configuration data which includes automatically re-enabling the MPC boot timer.

Disabling the boot timeout using Linux commands

To disable the boot timeout using Linux commands:

1. Connect a crossover cable from the Services laptop into the Services port on the MPC.
2. From a command window, type **`arp -d 192.11.13.6`**. Press **Enter**.
3. On the Services laptop, click on the **Putty** desktop link or select **Start** > **Programs** > **PuTTY** > **PuTTY**.

   The system displays the **PuTTY Configuration** window.

4. In the **Host Name (or IP address)** field, type **`192.11.13.6`**.
5. In the Protocol area, click **SSH**.
6. In the **Port** field, type **`10022`**.
7. Click **Open**.

Note:

The system displays the **PuTTY Security Alert** window the first time you connect to the SAMP with this version of PuTTY.

8. If this is the first time that you connect to the MPC, click **Yes** to accept the server's host key. Otherwise, go to step 9.

   The system displays the **PuTTY** window.

9. Log in as **craft**.

   The system prompt displays. For example, **craft@STA04410179:~$**

10. At the prompt, type **serverctrl boot timer disable**. Press **Enter**.

    The system responds with an OK message.

11. Type **serverctrl**. Press **Enter**.

    Note:

    The system message should indicate that the boot timer is disabled.

    The system responds with the following messages.

```
Power On

Server Not Operational

Reset Deasserted

Boot Timer Disabled
```

Password protection

The MPC's default configuration includes two logins - craft and rasaccess. Prior to loading Remote Feature Access' (RFA) authentication file, these may be used by either Avaya Services or BusinessPartners. The remote access (rasaccess) password is necessary when accessing the server through the modem to establish a PPP session.

Upon installing the RFA authentication file, the S8400's default static passwords are changed automatically for security reasons. Services personnel should be aware that the rasaccess password changes every time an authentication file is loaded. Since the process relies on the Automatic Registration Tool (ART) to manually train Avaya's connect tool when the rasaccess password has been changed, it is imperative that the technician rerun ART whenever a new authentication is loaded.

BusinessPartners must create an alternate system login. The recommended system login is **dadmin**, with a password of the BusinessPartner's choice. The BusinessPartner may choose to create a PPP login for themselves. They must be cautious about utilizing modem access, however, as doing so blocks product alarming and also blocks Avaya Services from remotely

fixing problems. If the BusinessPartner forgets to create logins or loses their login/password, they will not be able to access the MPC nor remotely access the server. Upon request, the BusinessPartner's login/password can be reset for a fee by Avaya's Technical Consulting - System Support team (U.S.-based BusinessPartners at 1-800-225-7585) or Regional Service Centers (non-U.S.).

Updating the MPC firmware

Occasionally new firmware for the MPC is available at the Avaya Support Website (http://support.avaya.com).

This section contains these topics:

- Determining the latest firmware version on page 121
- Downloading new firmware to the staging area on page 122
- Accessing the server on page 122
- Copying and installing MPC firmware to the server on page 123

Determining the latest firmware version

To determine the firmware on the MPC:

1. From the server, open a command line (for example, telnet) and type **`sampcmd samp-update status`** and press **Enter**.

   The system displays information similar to the following example:

   ```
   craft@server-name> sampcmd samp-update status
   Serial Number: IN8400_EMBEDDED
   Version ID: AVAYA_TN8400 2_0
   Boot type: committed
   Active Kernal/Root 2/6
   Committed Kernel/Root: 2/6
   U-Boot boot command: run k2r6; run netboot
   ```

2. The **Version ID** line lists the latest firmware load on the server.
3. On a Web browser, go to http://support.avaya.com.

   The system displays the **Avaya Support** window.
4. Click on **Download Center**.
5. Locate the MPC firmware update and check the version number against the version on your server.

Downloading new firmware to the staging area

CAUTION:

Make sure that you want to upgrade the MPC firmware before you initiate the download. Once you have successfully downloaded and saved the new firmware to the MPC, you cannot cancel the upgrade.

To upgrade the MPC firmware:

1. Go to the Avaya Support Website (http://support.avaya.com). Follow the **Software & Firmware Downloads** link and subsequent links.
2. Find the section for the firmware vintage you want. Unless otherwise instructed, choose the highest vintage.
3. Be sure to read that vintage's ReadMe file before downloading the image file(s).
4. For each image file to be downloaded:
   a. Click on the image filename.
   b. Save this file to disk in a convenient directory.

Tip:

Remember the full path to the firmware image. You will need this information later.

Accessing the server

To access the server:

1. You can access the server by any of these methods:
   a. Logging into the server using the IP address of the server.
   b. Connecting the to the services port on the server, opening a Web browser and typing `http://192.11.13.6` in the **Address** field and pressing **Enter** to bring up the logon Web page.
   c. Connecting through the network, opening a Web browser, typing the server name or IP address of the server in the **Address** field, and pressing **Enter**.
2. Log in as **craft**.
3. When asked whether to suppress alarms, click **Yes**.

   The system displays the Home window.
4. Click **Launch Maintenance Web Interface** to get to the Main Menu.

Copying and installing MPC firmware to the server

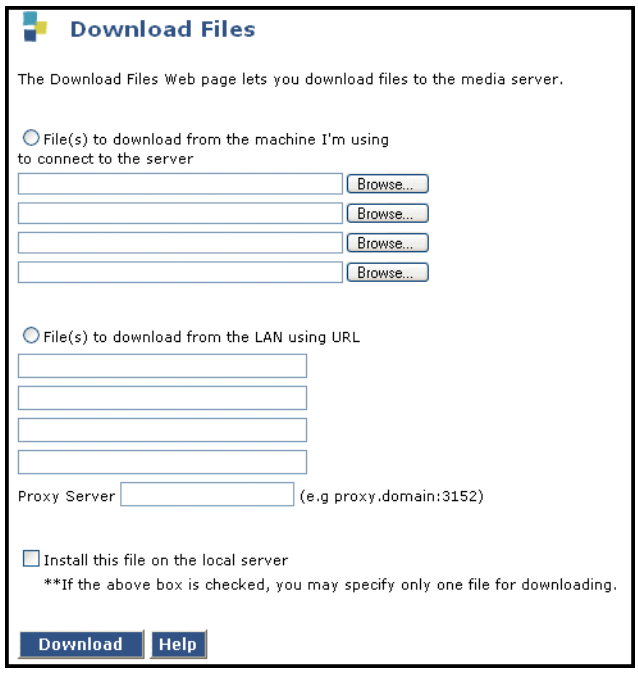
CAUTION:

Make sure that you want to upgrade the MPC firmware before you initiate the update. Once you have successfully downloaded and installed the new firmware into a MPC, you cannot cancel the upgrade.

To copy the firmware to the server:

1. On the Web browser, under Miscellaneous, click **Download Files**.

   The system displays the **Download Files** window.



2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the **Choose File** screen on your computer. Find the firmware that you downloaded from the Avaya Support Website.
4. Click **Download** to copy the file(s) to the server.
5. Telnet or SSH to the server and log in as **craft**.
6. Type **`sampupdate`** and press **Enter**.

Note:

This upgrade takes several minutes; at times, there may be no progress indicators. After the MPC accepts the new firmware, it reboots.

If the system encounters a problem during the update, an error message displays. Check the **sampupdate** output and log files that are available through the modem/services port. Each upgrade produces a unique log file that contains more information about why the upgrade failed.

Chapter 4: Server initialization, recovery, and resets

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

- S8700 Initialization on page 125
- Automatic trace-route on page 127
- Network recovery on page 137
- System resets on page 219

S8700 | 8710

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 (for example, 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. Duplication Manager (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 packet control driver (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.

Automatic trace-route

S8300 / **S8500** / **S8700 | 8710**

In order to diagnose network problems, especially to determine where a network outage exists, Communication Manager initiates an automatic trace-route command when the connectivity between a server and its port networks, media gateways, or IP trunks is lost. This includes:

- IPSI-connected port networks (**S8500** / **S8700 | 8710** only)
- IP trunks (signaling groups: **S8500** / **S8700 | 8710** only)
- All media gateways

Note:

The Avaya S8300 Media Server does not support port networks. And, while the S8300 can have IP trunks, it does not monitor their status.

This feature does not apply to the csi, si, r platforms.

Depending on the type of link failure, Communication Manager determines whether to initiate the trace-route command from a CLAN circuit pack or from the native NIC.

Hardware/software requirements

This feature requires

- CLAN circuit pack TN799B or above
- Communication Manager, Release 2.2 or later

Note:

This feature defaults to “on” for upgrades/new installations to Release 2.2.

Monitored links

The automatic trace-route feature monitors the following links for failures:

- **Server-to-media gateway**: the link between the server acting as a gateway controller and any media gateway. A link to a media gateway that is in busy-out or disabled state is not a failed link.
- **Server-to-port networks**: the link between the active server and any IPSI-connected port network. A link to a port network that is in busy-out or disabled state is not a failed link.
- **Server-to-IP trunks** (H.323 signaling groups): the link between the server acting as a gatekeeper and any H.323 signaling group. Subsequent call failures using the same H.323 signaling group do not generate new log entries until that H.323 signaling group has successfully processed a call. The maintenance subsystem (except **S8300**) can also identify a failed link whenever any of these Error Types against the H323-SGRP maintenance object occur:
  - Error Type 257: ping test failures
  - Error Type 513: ping test excessive delay times
  - Error Type 770: excessive latency and packet loss from the Media Processor (maintenance object H323-SGRP Error type 770).

    A link to an H.323 signaling group that is in busy-out or disabled state is not a failed link.

Note:

A call connection that is blocked from completion over a WAN link through the Call Admission Control Bandwidth Limitation feature is not a failed link and does not generate an automatic trace route over that link.

Configurations

The automatic trace-route feature works with the following configurations:

- **Enterprise Survivable Servers** (ESS): applies to the connections between the ESS and those port networks, media gateways, and signaling groups that the ESS is actively controlling.
- **Local Survivable Processor** (LSP): applies to S8300 or S8500 (through the Processor Ethernet interface) media servers functioning as a LSP and the media gateway connections that the LSP is actively controlling.

Administration

With proper permissions you can turn the automatic trace-route feature on and off from the system access terminal (SAT):

1. Type **`change system-parameters ip-options`** and press **Enter**.

   The **IP-Options System Parameters** form displays.

IP-Options System Parameters form

```
change system-parameters ip-options

                         IP-OPTIONS SYSTEM PARAMETERS

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

 RTCP MONITOR SERVER                                AUTOMATIC TRACE ROUTE ON
         Default Server IP Address: 192.168.15 .84            Link Failure? y
               Default Server Port: 5005
  Default RTCP Report Period(secs): 5

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

 H.248 MEDIA GATEWAY                 H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5      Link Loss Delay Timer (min): 1
                                        Primary Search Time (sec): 15
```

2. To enable the automatic trace-route command set the **AUTOMATIC TRACE ROUTE ON Link Failure** to **y**.

   To disable the automatic trace-route command set the **AUTOMATIC TRACE ROUTE ON Link Failure** to **n**.

   Note:

   If you disable the feature, any automatic trace-route currently in progress finishes, and no subsequent trace-route commands are launched or logged (the link failure buffer is cleared).

3. Press **Enter** to submit the form.

Command results

The logged results of the trace-route command can help you determine network outages that cause link failures and is available:

- On the Maintenance Web pages
- In the Linux log files

If you initiate a trace-route from the system access terminal (SAT), the results are not logged but appear on the SAT form after the command is issued. See trace-route in *Maintenance Commands Reference (03-300431)* for information about how to interpret the report. See Conditions and interactions on page 135 for command precedence information.

Maintenance Web pages

To view the results of the **`trace-route`** command in the Maintenance Web Pages:

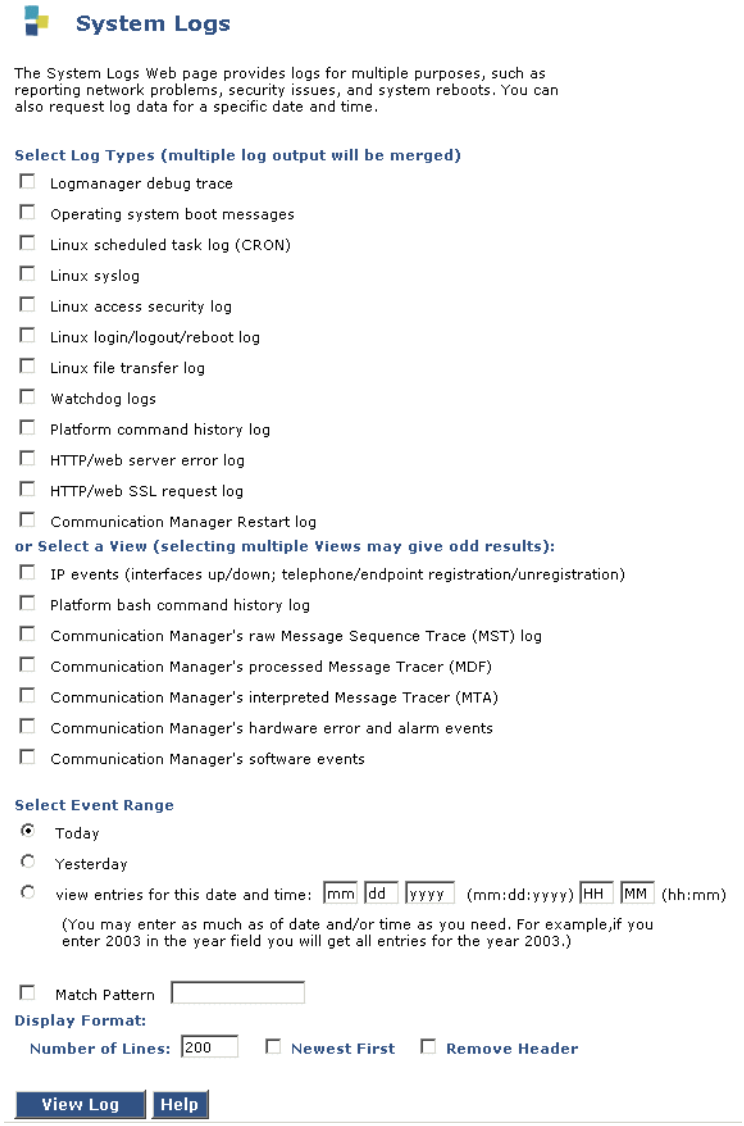
1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

2. From the left side select **Diagnostics > System Logs**.

   The **System Logs** page (Figure 9: System Logs page on page 131) displays.

Figure 9: System Logs page



3. In the **Select Log Types** section select **IP Events**.
4. Click on the **View Log** button at the bottom of the page.

   The View Log page displays 200 lines of the most recent log entries.
5. The Interpreting the Web interface log entries section describes the various log entry types.

Linux log files

To view the results of the trace-route command in the Linux log file:

1. At the command line interface type:
   - **logv IPEVT** to display all IP events
   - **logv IPEVT today** to view the IP events log for the current day
   - **logv TR_** to view the automatically-launched trace-route log
   - **logv TR_IPSI** | **TR_SG** | **TR_MG** to see the IPSI, Signaling Group or media gateway logs, respectively.
2. The Interpreting the Web interface log entries section describes the entries associated with the trace-route command.

Interpreting the Web interface log entries

Each line of the log consists of common information available on any line of the tracelog followed by event-specific information. The beginning of each line of the IP events log is exactly the same as those of any line on the tracelog. The generic information is distinct from the failure-specific information in that it is separated by colons(:) as in the following example:

```
20030227:000411863:46766:MAP(11111):MED:
```

Interpret the information as follows:

- **20030227** is the date (February 27, 2003)
- **000411863** is the time (00 hours, 04 minutes, 11 seconds, 863 milliseconds (ms) or 00:04:11 AM).
- **46766** is the sequence number of this entry.
- **MAP(11111)** is the name and number of the process generating the event.
- **MED** is the priority level (medium).

Following the generic information the following information appears in brackets [] for all trace-route commands, whether successful or not:

- Source board location
- Source IP address
- Network region

- IPSI number (for port network link failures), media gateway number (for media gateway link failures), or signaling group number (for signaling group failures)
- Destination IP address
- Successful hops: information about successful hops along the route:
  - Hop number
  - IP address of hop
  - Times (in ms) to reach that hop (3 separate time values)
- Unsuccessful hops: information about unsuccessful hops along the route:
  - Hop number
  - IP address of hop
  - Times – indicates “*” to indicate a failed hop or very large time periods
  - Error code indicating reason for failed hop (same as that returned from a user-initiated trace-route command)
  - Additional information specific to aborts of the trace-route
  - Tag indicating that automatic trace-route has been aborted and a reason

Examples of specific failure events are interpreted in the following sections:

- Media gateway link failures
- Port network link failures
- IP trunk (H.323 signaling group) link failures
- Failed hop
- Aborted trace-route

Note:

Even though some the examples below show wrapped lines of text, both the Web page and the Linux log display one line per entry.

Media gateway link failures

In addition to the generic information, the log shows an example of a media gateway link failure:

```
[TR_MG board=01A06 ip= 135.9.78.112 net_reg= 1 mg= 1
dest= 135.9.71.77 hop= 1 135.9.78.254 2.000ms 3.000ms 2.000ms]
```

Interpret the information as follows:

- Brackets surround the failure-specific information
- Type of IP event (TR-MG): a trace-route for a link failure to a media gateway
- Source board location (01A06)
- Source IP address (135.9.78.112)

- Network region number (1)
- Media gateway number (1)
- Destination IP address (135.9.71.77)
- Hop number (1)
- Hop IP address (135.9.78.254)
- Three times in milliseconds (ms) for the three different attempts made at each hop along a route (2.000ms, 3.000ms, 2.000ms)

Port network link failures

In addition to the generic information, the log shows an example of a port network link failure and includes a tag for the type of IP event in brackets:

```
[TR_IPSI board=PROCR ip= 172.28.224.18 net_reg= 1 ipsi= 2
dest= 135.9.71.75 hop= 1 135.9.78.254 2.000ms 3.000ms 2.000ms]
```

Interpret the information as follows:

- Brackets surround the failure-specific information
- Type of IP event (TR_IPSI): a trace-route for an IPSI link failure to a port network
- Source board location (PROCR): the processor Ethernet (native NIC)
- Source IP address (172.28.224.18)
- Network region number (1)
- IPSI number (2)
- Destination IP address (135.9.71.75)
- Hop number (2)
- Hop IP address (135.9.78.254)
- Three times in milliseconds (ms) for the three different attempts made at each hop along a route (2.000ms, 3.000ms, 2.000ms)

IP trunk (H.323 signaling group) link failures

In addition to the generic information, the log shows an example of an IP trunk link failure:

```
[TR_SG board=01A08 ip= 135.9.78.112 net_reg= 1 sg= 1
dest= 135.9.71.77 hop= 1 135.9.78.254 2.000ms 3.000ms 2.000ms]
```

Interpret the information as follows:

- Brackets surround the failure-specific information
- Type of IP event (TR_SG): a trace-route for a link failure to an IP trunk
- Source board location (01A08)
- Source IP address (135.9.78.112)
- Network region number (1)

- Signaling group number (1)
- Destination IP address (135.9.71.77)
- Hop number (1)
- Hop IP address (135.9.78.254)
- Three times in milliseconds (ms) for the three different attempts made at each hop along a route (2.000ms, 3.000ms, 2.000ms)

Failed hop

The following examples illustrate failed hops along the route:

```
[TR_IPSI board=PROCR ip= 172.28.224.18 net_reg= 1
 ipsi= 2 dest= 172.28.224.2 hop= 1  172.28.224.18
   2965.401ms !H  2997.313ms !H  3000.750ms !H]

[TR_IPSI board=PROCR ip= 172.28.224.18 net_reg= 1
     ipsi= 1 dest= 172.28.224.1 hop= 1  * * *]

[TR_IPSI board=PROCR ip= 172.28.224.18 net_reg= 1
     ipsi= 1 dest= 172.28.224.1 hop= 2  * * *]

[TR_IPSI board=PROCR ip= 172.28.224.18 net_reg= 1
     ipsi= 1 dest= 172.28.224.1 hop= 3  * * *]
```

The example shows the case for a port network failure; other failures would be analogous. Depending on the circumstances, sometimes very long times are shown along with error codes, if known. In other circumstances, the times are shows as “*.”

Aborted trace-route

The following examples show an aborted trace-route:

```
 [TR_SG board=01A06 ip=   135.9.78.112 net_reg=   1 mg=
1 dest=    135.9.71.77 hop= Aborted due to contention!]
 [TR_SG board=01A06 ip=   135.9.78.112 net_reg=   1 mg=
1 dest=    135.9.71.77 hop= Aborted due to socket close!]
```

This example shows an aborted trace on an IP trunk link failure: once for contention with a SAT-initiated trace-route and the second time for the socket closing.

Conditions and interactions

The following conditions and interactions apply to the automatic trace-route feature:

- If multiple links are lost at the same time, only a limited number of automatic trace-route commands are launched.
- 10 trace-route requests are held in a buffer at any given time; all other links failures that exceed the buffer size are dropped.

- Only one automatic trace-route command is launched and completed at a time per system. A new automatic trace-route cannot begin until the previous automatic trace-route completes or aborts. As soon as an automatic trace-route command is issued for a particular failed link, that entry is removed from the failed link buffer.
- The automatic trace-route command aborts when:
  - Encountering failed hops, that is, all three packets for that hop are unanswered (three asterisks).
  - Some other process (for example, a user-initiated trace-route command) takes precedence.
  - Communication Manager resets (Level 2 or higher); no further automatic trace-routes are launched during a reset, and the failed link buffer is cleared.
  - The Linux operating system (OS) crashes; any automatic trace-route commands in progress on CLAN circuit pack or the native-NIC abort, and the failed link buffer is cleared.

  Note:

  Aborts due to a Linux OS crash are not logged in the IP events log; the Linux OS logs should indicate that the OS restarted.

  - **S8700 | 8710** only: the servers interchange (not logged in the IP events log); other areas of the log files should indicate the server interchange, which also includes a warm restart (reset system 1). The failed link buffer is retained through an interchange, and trace-route commands in the buffer are launched after an interchange or warm reset.

    Since the log files are resident on each server, a server interchange means that the log file being written to also changes. Only the entries that occur while the given processor is active appear in that server's log. In order to get a complete history you must go to each server and view the respective logs.
  - The command is not completed within predetermined time period:
    - CLAN: 1 minute
    - Native NIC: 2 minutes

  Note:

  Aborted trace-route commands are not restarted for CLAN circuit packs or native-NIC interfaces.

  - The link fails and then before the automatic trace-route command can be run over the given CLAN interface, the CLAN interface is taken out of service, then there is no way to actually perform the trace-route. By the time the CLAN interface comes back into service, the link failure may no longer be an issue and hence, there is no attempt to retry that trace-route.
- **S8300** and **S8500** only: RAM disk configuration supports server reliability by partially surviving a disk crash. In this situation, even though Communication Manager is running on the RAM disk, there is no disk to which the system can write the results of the automatic trace-route.

Network recovery

When the media gateway and the primary server from which it gets its call control lose connection with each other, Avaya's network recovery strategies immediately begin to either reconnect with the primary server or to find alternate call controllers.

Figure 10 depicts the recovery timers that work in concert to reroute network connections.

Figure 10: Recovery timers and their interactions

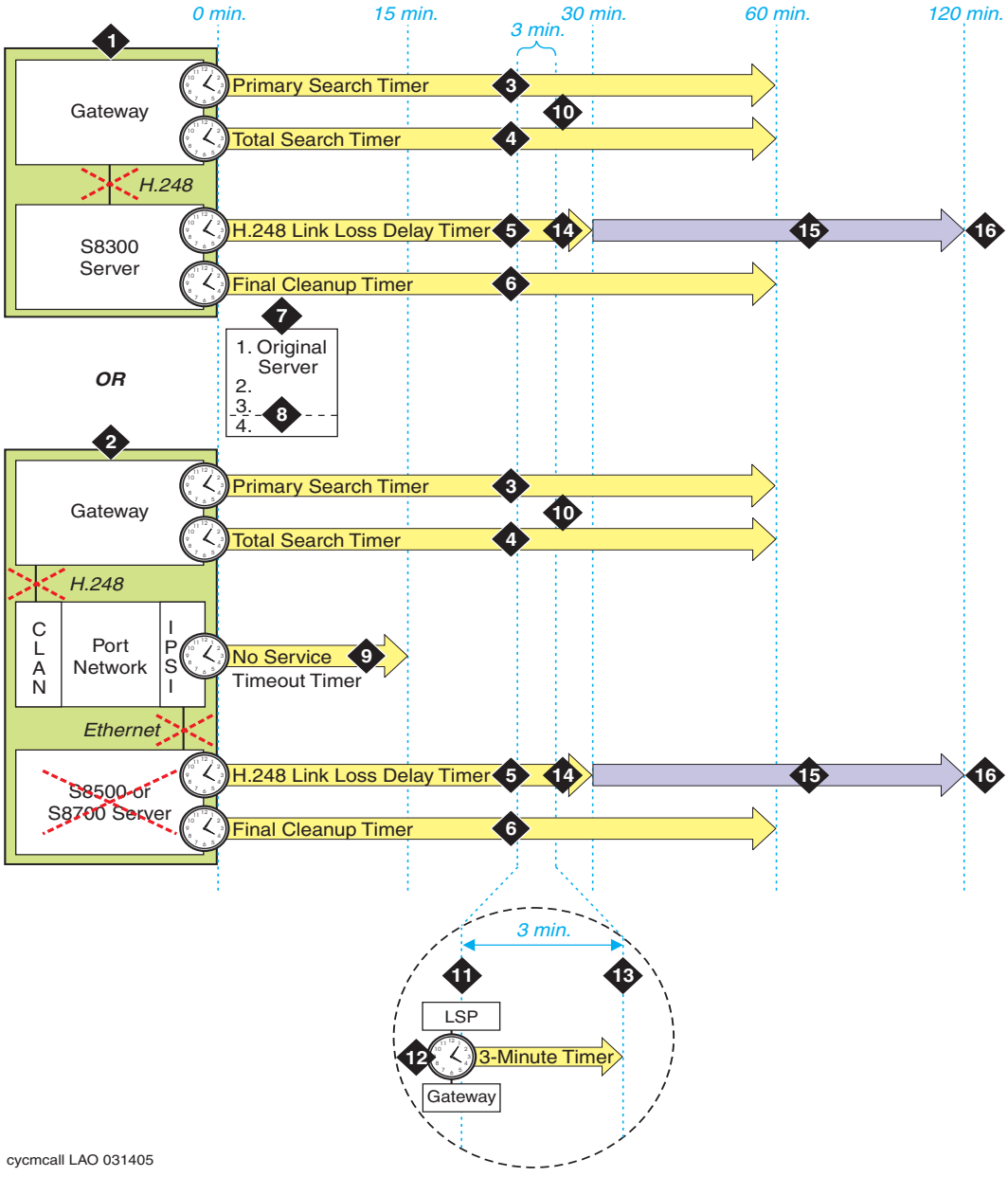


Figure notes:

1. **S8300**: H.248 link between the server and the media gateway is broken.
2. **S8500 (Processor Ethernet interface) or 8700 Series**: If the Ethernet connection is broken between the server and the port network or the server fails, the Enterprise Survivable Server (ESS) feature, if available, is launched, starting the No Service Timeout Timer (NSTT; see Note 9)

   Note: if the Ethernet connection is broken, then the H.248 signaling connection to the gateway is also broken.
3. Primary Search Timer (PST, see H.248 Link Recovery processes) begins on the media gateway
4. Total Search Timer (TST, see H.248 Link Recovery processes) begins on the media gateway
5. Link Loss Delay Timer (LLDT, see Link Loss Delay Timer)
6. Final Cleanup Timer (FCT, see Final Cleanup Timer)
7. Media Gateway Controller list (MGC). The first element in this list is always the primary server; the fifth element is for G250 SLS (survivable-call-engine).
8. Transition point (see Note 8 and Administering the Media Gateway)
9. No Service Timeout Timer (NSTT) on the IPSI (3-15 min., default is 5 min.) starts if available, when the IPSI loses contact with the main server.
10. If the Primary Search Timer (PST) expires before the gateway can re-establish the link to the alternate resources that are above the Transition Point in the Media Gateway Controller (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.

    If the gateway cannot re-establish the link to any of the resources below the Transition Point, then it starts over at the top of the MGC list and continues to the end, making only one reconnection attempt to each element in the list. This continues until the Total Search Timer (TST) expires.
11. Auto Fallback to Primary starts a 3-minute, administrable timer that checks for network stability before the server accepts the registration requests from the media gateway.
12. Auto Fallback to Primary: media gateway connects to LSP before the Link Loss Delay Timer (LLDT) expires.
13. Auto Fallback to Primary: media gateway sends registration requests to primary server at 30-second intervals (similar to "keep alive" signals). Server gives gateways without LSP service priority to those with LSP service; see Local Survivable Processor (LSP).
14. Link Loss Delay Timer (LLDT) expires, Connection Preserving Failover/Failback and Standard Local Survivability (SLS) on the G250 media gateway begin.
15. Connection Preserving Failover/Failback starts as soon as the media gateway migrates to another server.
16. Connection Preserving Failover/Failback's Final Cleanup Timer (FCT) expires.

Connection Preserving Failover/Failback

The Connection Preserving Failover/Failback for H.248 gateways preserves existing bearer (voice) connections while a H.248 media gateway migrates from one Communication Manager server to another because of network or server failure. However, users on connection-preserved calls cannot use such features as Hold, Conference, or Transfer, etc. In addition to preserving the audio voice paths, Connection Preserving Failover/Failback extends the time period for recovery operations and functions during Avaya's complementary recovery strategies:

- H.248 server-to-gateway Link Recovery
- H.323 gateway-to-endpoint Link Recovery

- Auto Fallback to Primary
- Local Survivable Processor (LSP)
- Enterprise Survivable Server (ESS)

If two parties are on a call that is routed through an H.248 media gateway and the network connection carrying the media signal to the main server is lost, the voice (bearer) channel between the two users remains intact, and the two users can continue talking, unaware that the network connection is down. Even though the two parties can talk to each other, they cannot put the call on hold or conference in another party, those telephony features are not allowed. Avaya's network recovery strategy includes the Connection Preserving Failover/Failback feature to ensure that the new server to which the gateway connects retains calls in progress.

Topics in this discussion include:

- Starting Connection Preserving Failover/Failback
  - Calls preserved/not preserved or available
- Connection Preserving Failover/Failback process
- New or modified functionality
  - New/old servers
  - Media gateway and VOIP media module
- VoIP monitoring
- Timers

Starting Connection Preserving Failover/Failback

Connection Preserving Failover/Failback begins with the loss of the H.248 network connection between the gateway and the primary server. During the time that the gateway migrates to another server for its call control, Connection Preserving Failover/Failback preserves the voice path and after it migrates to the new server. Loss of the H.248 network connection causes the media gateway to failover or failback to a new server:

- Main server to LSP or ESS
- Main server back to itself after system reset
- One LSP to another LSP
- One ESS to another ESS
- LSP to an ESS
- LSP/ESS back to main server after expiration of the Link Loss Delay Timer that clears out calls on the server.

Calls preserved/not preserved or available - Connection Preserving Failover/Failback preserves:

- Stable calls (talk path already established), including:
  - Analog stations and trunks
  - DCP stations
  - Digital trunks
  - IP stations that use media gateway resources
  - ISDN-PRI trunks
    - D-channel on the media gateway needs mapping to the B-channel for reconstruction
    - Stable Facility Associated Signaling (FAS) calls are preserved; signaling and bearer channels migrate together
    - Non-Facility Associated Signaling (NFAS) calls can have signaling and bearer channels on different media gateways. Avaya recommends that the media gateways be physically co-located and administered to migrate together to the same set of LSPs and in the same order.
  - Inter-gateway calls using Inter-Gateway Alternate Routing (IGAR)
- Conference calls, however all parties in the conference drop whenever any party drops

Call features (for example, Hold, Transfer, Drop, etc.) are unavailable on preserved connections. Users attempting to invoke any of the call features receive denial treatment. Callers can make new calls, but only after hanging up from an old call.

Connection Preserving Failover/Failback *does not* preserve:

- Calls on hold or listening to announcements or music (not considered stable calls).
- ISDN BRI calls
- IP trunk calls (SIP, H.323)
- Calls on hold (soft or hard)
- Calls with dial tone
- Calls in the ringing state
- Calls in the dialing state
- Calls in vector processing
- Calls in ACD queues
- Calls on port networks that failover/failback

Note:

See Software/firmware versions on page 144 for compatibility issues between the server and media gateway.

Connection Preserving Failover/Failback process

Connection Preserving Failover/Failback functions within the larger context of network recovery, which also includes the following features/functionality:

- H.248 Link Recovery (previously released)
- Enterprise Survivable Servers
- Auto Fallback to Primary for H.248 Gateways
- SLS (Survivability.o) for G250 Media Gateways

New or modified functionality

This section compares the new server, gateway, and VoIP media module functionality resulting from Connection Preserving Failover/Failback development.

New/old servers - The new server functionality is changed to:

- Send additional connection information down to the H.248 gateway for call setups
- Receive connection information from the H.248 gateways in reconstruction mode
- Place the new gateway into service by first finding out which connections need to be preserved
- Tear down calls that cannot be preserved (for example, disconnects or calls that no longer have a voice path). See Calls preserved/not preserved or available on page 140 for more information.

Old server functionality is different depending on when the gateway re-registers with it:

- If the media gateway re-registers with the old server *before the Link Loss Delay Timer (LLDT) expires*, the old server fully preserves the calls that it is already aware of and reconstructs only those calls that the new server (for example, an LSP) started.
- If the media gateway re-registers with the old server *after the Link Loss Delay Timer expires* then the gateway reconstructs calls, since the old server has no knowledge of them.

There is more information about the Link Loss Delay Timer on page 143.

Note:

In an ISDN NFAS scenario, media gateways with D-Channels migrate to the new server while the B-Channels might remain at the same server. The new server does not drop the B-Channels on active (stable) calls in response to D-Channel going out of service.

Media gateway and VOIP media module - The H.248 media gateway and VOIP media module functionality has changed to:

- Receive additional connection information from the server for call setups
- Send connection information to the server when connected to a new server
- Monitor the physical termination status of phones in calls being connected or disconnected
- Monitor the bearer channel for voice activity (see VoIP monitoring on page 142)
- Send the physical terminations' connection status and the bearer channel status for the ephemeral (transitory) terminations to the new server

Earlier when the LLDT expired, all physical ports on the media gateway were removed, resulting in dropped calls. Now the new server reconstructs the part of the call that migrated with the media gateway, and the primary server keeps intergateway calls (IGC) up until the last party hangs up or when the media gateway detects the VOIP channel is not in use (see VoIP monitoring on page 142).

VoIP monitoring

The VoIP monitoring mechanism is based on the assumption that RTCP is enabled on all endpoints and that the media gateway should receive RTCP/RTP packets for all the ephemeral terminations that are in the active context at the time of call setup. The channel is released If there is no VoIP activity on the channel, freeing these resources.

The VOIP engine detects the VoIP activity using these criteria:

- Detection on the channel is enabled only if the far end has sent at least one RTCP packet during the call.
- The VoIP media module declares a channel inactive when
  - The channel has received RTCP packets at some point, AND
  - No new RTCP packets are received for 150 seconds, AND
  - No RTP packets are received during the same time interval
- If the VOIP channel is used for a T.38 fax call, the far end might have sent a RTCP packet during the period in which the voice call is converted to a fax call. However, once it becomes a fax call, there is no RTCP or RTP traffic. In this case the VoIP engine disables VOIP monitoring on that channel and notifies the media gateway.

The Network Region form has a **RTCP Reporting Enabled?** field that indicates if RTCP Reports should be sent to a special server, such as for the VMON tool (Figure 11).

Figure 11: IP Network Region form

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location: 1               Home Domain:
    Name: S8700MC Lab
                               Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS               Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                          IP Audio Hairpinning? y
UDP Port Min: 1100
UDP Port Max: 1229                   RTCP Reporting Enabled? y
                             RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS       Use Default Server Parameters? y
 Call Control PHB Value: 34
        Audio PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Important:
RTCP packets are always sent peer-to-peer no matter how this field is administered.

Timers

There are two main timers that impact Connection Preserving Failover/Failback:

- Link Loss Delay Timer
- Final Cleanup Timer

Link Loss Delay Timer - The Link Loss Delay Timer (LLDT; 1-30 minutes; default is 5 minutes) is an administrable timer used in the H.248 Link Recovery feature. This timer starts when the Communication Manager server detects loss of connectivity with a media gateway. It is canceled and Communication Manager-media gateway state is resynchronized if the media gateway reconnects with the server before the timer expires. If the LLDT expires and the media gateway has not yet come back, the server performs a board removal of all the inserted boards belonging to that media gateway. As a consequence, all physical terminations related to that media gateway are also removed from calls.

The Connection Preserving Failover/Failback development has changed the LLDT behavior slightly: earlier, when the LLDT expired for a media gateway, the physical terminations on that media gateway were removed from a call. If that leaves only a IGC ephemeral termination and one other termination in the call, then that call is considered a one-party call and torn down. As part of Connection Preserving Failover/Failback these one-and-a half calls are preserved until

- VOIP channel inactivity is detected on the IGC termination, or
- The other termination hangs up.

Final Cleanup Timer - The Final Cleanup Timer (FCT) is a long (120 minute), per-gateway timer that is used for cleaning up preserved, new-server connections that did not receive disconnects. This timer starts on a server when a media gateway migrates to it. When it expires any preserved connections that do not have disconnect supervision are removed. These include:

- IP Stations and IP Trunks in a reconstructed call
- PRI B-Channels in a call for which corresponding D-Channels are not under the control of the server
- Trunks with no disconnect supervision

Software/firmware versions

Note:

Connection Preserving Failover/Failback cannot work properly unless the Communication Manager software on the server, the firmware on the H.248 media gateway, and the firmware on the VOIP media module are compatible.

- Avaya Communication Manager, Release 3.0 or later.
- Release 3.0 or later media gateway firmware and VOIP media module firmware

Note:

Media gateways that contain connection preservation firmware work with servers running older versions of Communication Manager, however, connections *are not* preserved. Likewise, media servers that contain connection preservation software work with media gateways running older versions of media gateway firmware, although these connections *are not* preserved.

Note:

There is no customer option form entry nor any license file implications for the Connection Preserving Failover/Failback feature, which is always enabled and available.

Platforms

Connection Preserving Failover/Failback is supported on:

- S8300 Media Server
- S8500 Media Server
- S8700 series Media Servers
- All H.248 Media Gateways

Backward-compatibility caveats include:

- Newer Media Gateways work with older servers, but no connection preservation.
- Older Media Gateways work with newer servers, but no connection preservation.
- Older VoIP media modules do not do VoIP monitoring for active calls.

Cross-Product compatibility

- Terminals

  No change to any terminal's firmware is needed for this feature.

- Adjunct Switch Applications Interface (ASAI)

  ASAI loses the ability to perform third-party call control for a call on a media gateway if the gateway loses its connectivity to the server.

- Voice Mail Adjuncts (AUDIX, Intuity, Octel)

  A stable bearer connection between a voice mail adjunct and an endpoint are preserved just like any other stable call.

- Call Detail Recording (CDR)

  Call Detail Recording is only updated for calls on the original server. During a failure condition, the original server marks the calls as being torn down after the Link Loss Delay Timer has expired and updates CDR records that the calls are completed. The server does not update CDR records for the reconstructed calls.

- Call Management System (CMS)

  The links to the Call Management System are not preserved in a failover of a media gateway to another server.

- Property Management System (PMS)

  The links to the PMS system are not preserved in a failover of a media gateway to another server.

- Voice Response Systems (Conversant)

  The links to a voice response system are not preserved in a failover of a media gateway to another server.

- Communication Manager Application Programming Interface (Communication ManagerAPI)

  Applications running on the Communication ManagerAPI server connect with Communication Manager through an IP softphone-like interface. Hence, an individual instance of an application might end up in “connection preservation” mode, where no Communication Manager features other than disconnects are allowed.

Feature interactions

Connection Preserving Failover/Failback affects these features:

- Auto Fallback to Primary

  To avoid thrashing and probable CPU spikes, the primary server will not allow the auto fall back of the media gateway until it receives registration requests for at least six consecutive tries (which should take about three minutes). This would avoid any thrashing.

- Call Admission Control - Bandwidth Limits (CAC-BL)

  The Call Admission Control feature places limits on calls that are carried over WAN links between IP network regions. Calls that exceed those limits are denied and instead sent over PSTN facilities through IGAR or delivered to alternative destinations through call coverage. This requires that the server keep track of the number of connections and the bandwidth used for connections going between bandwidth regions. During fail-over conditions:

  - Both the old and new servers only have partial knowledge of the number of calls and the bandwidth used.
  - Reconstructed calls are not counted toward the bandwidth count for Call Admission Control.

- Drop

  The drop button is a fixed feature button on some telephone sets, and is administrable on other types of phone sets. When used in conjunction with Connection Preservation, pressing the drop button results in dropping a 2-party call but has no effect for a conference call. This is true regardless of whether the drop button is a fixed or an administrable button.

- Enterprise Survivable Server (ESS)

  If the media gateway was connected to the server through a CLAN, and the port network the CLAN is on fails over to an ESS server, then the IP phone attempts to register with the new server, even if it is on a call.

  This is similar to a scenario where the server goes through a reboot and it would not want the IP phone to register. This is prevented by making the IP phone send a flag in RRQ which is checked against user record to see if the user is on a call. If the user record indicates there is no call, the registration is denied.

  In the case of reconstruction the server checks the IP phone service state along with the check for existence of a call associated with the user to determine if it should deny registration or not. If the IP phone indicates it does not have any call, and the server thinks it is on a call, the call is dropped, and the IP phone is allowed to register.

If a port network fails to an ESS server, currently the port network calls are not reconstructed, whereas the media gateway connections are reconstructed. If there is a call between the PN and media gateway, only the media gateway part of the call is reconstructed.

- E911

  An E911 call is treated just like any other call in that it is preserved if possible (assuming the bearer path stays up) during a media gateway failover to a new server.

- Far-end Mute

  The Far-End Mute feature allows a user to mute a noisy far-end trunk participant in a conference call. Both the conference display feature button and the far-end mute feature button must be administered. The user cycles through a list of the participants on the conference call until they get to the party they want to mute. They then select the far–end mute feature button to mute the party.

  Individual participants in a conference call that were muted by the far-end mute feature are still muted during connection preservation. However, these participants can no longer be unmuted when the call is in a connection preserved case.

- Hold

  Calls on hold will not be preserved under the connection preservation feature, as described in earlier sections. In addition, calls on hold will not be monitored to see if there is active VOIP traffic.

- H.248 Link Recovery

  The H.248 Link Recovery feature still applies to MGs that lose the link to the server and then re-register directly with that server (and no other server) before the Link Loss Delay Timer expires.

- H.323 stations

  Today an IP phone that is on a call tries to get back to the primary server if it loses its signaling link (when TCP keep alive fails) to the server. If the server is aware of the call it would allow the IP phone to register; otherwise it rejects the registration until the IP phone is not on any call.

  Two H.323 IP stations can be connected to each other in two ways:

  - Shuffled call: In this scenario the RTP streams from one phone terminate on the other phone. This type of call setup does not require any media gateway VOIP resources. And therefore the new server would not know about the call.
  - Unshuffled call: In this case the RTP streams from each phone terminated on a Media Processor resource (media gateway-VOIP or PN Prowler). And the Media Processor re-directs the RTP streams to the destination phone. This type of connection configuration is used if trans coding is needed, or if one of the IP phone is in one network and the other is another network.

In this case the server is aware of the call, since this call is using the media gateway resources. The following are possible scenarios:

- The two party IP phones call is reconstructed before the IP phones try to register: When the IP phone registers, the phone would indicate the server about the call (through the “call Present” flag in RRQ). The server rejects the registration and asks the IP phone to register when it ends the call.
- The IP phones register before the call is reconstructed: The IP phone sends a “call Present” flag in RRQ and the server will not have any call for the call and therefore reject the registration (RRQ) and ask the IP phone to register when the call ends. The server can still go ahead create the call record for the IP phone as a part of call reconstruction. On the previous server (that is, the server media gateway was receiving service from before the failover), the call records are left as they are until either the user goes on hook or the server detects that the signaling channel to the IP phone/s is down. When the server detects the signaling channel outage it starts a timer to clear the call. This timer is administrable by the system administrator.
- Two IP phones (with shuffling turned on) are in a call with a DCP phone (or any physical) on a media gateway: The original server does not try to shuffle the IP phones in the call (even if the shuffling is turned on) if the server cannot signal to the media gateway. This applies to IP stations, IP trunks and IGCs.

Note:

This also applies if three IP entities (IP phone or IP trunk or IGC) are in a conference and an entity drops from the context. The server should not try to shuffle the remaining two IP entities if it cannot signal to the media gateway.

- Inter-Gateway Alternate Routing (IGAR)

  This feature allows the server to make use of trunk resources to make inter media gateway/ port network calls, if the IP bandwidth between network regions is not available. In a typical IGAR call the main server sets up two additional calls involving each trunk. When the call is reconstructed the new server constructs each side of IGAR connection as a separate call.

- IP phone shared control feature

  The Communication Manager server does not allow an IP Softphone that is sharing control of an IP Telephone to re-register until the IP Telephone has re-registered. The Communication Manager server allows an IP softphone that is sharing control of a DCP Telephone to re-register only after the DCP phone is in service. The IP Softphone is updated with the server’s knowledge of the DCP phone’s current button state.

- Multiple Level Precedence and Preemption (MLPP)

  MLPP is a feature set that was designed originally for Department of Defense private networks. This feature allows users to place calls at various levels of importance (called precedence) and preempt calls of lower importance.

  The Communication Manager server treats calls that are in a connection preserved state as routine calls but is also able to preempt a connection preserved call when MLPP is enabled.

- No-Hold Conference

  The No-Hold Conference feature allows a user to initiate and complete a conference call while still talking to the person on the original call. This feature does not put a party on soft-hold and no dial tone or ringing is heard. The original participants in a call that has invoked the no-hold conference feature to add in a new party remain on the call during connection preservation. The new party being dialed (using the no-hold conference feature) is dropped during connection preservation.

- H.323/SIP trunks

  In general H.323 and SIP trunks are dropped when the signaling channel is lost, meaning that calls on those trunks cannot be preserved.

- Administered connections

  The new server reconstructs administered connections. Any error messages that might be generated due to the new server trying to bring up an administered connection that is already up are ignored.

Modem Dial Backup

The modem dial backup (MDB) feature allows the gateway to utilize a modem to provide a redundant connectivity between a media gateway and IP phones on a small branch office and their main Communication Manager server at the headquarters or a regional branch office.

While gateways may have local survivability capabilities, either by an LSP or by the internal Standard Local Survivability (SLS) (G250 only), maintaining the connection with the Communication Manager server is always preferable, as many call features are lost when the network is fragmented.

For more information about the MDB feature, see *Administration of the Avaya G250 and the G350 Gateways*, 03-300436.

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 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 on page 150
- Conditions that trigger Link Recovery on page 150
- H.248 Link Recovery processes on page 150
  - General Link Recovery process on page 151
  - Call handling during recovery on page 152
  - Maintenance during recovery on page 153
- Link recovery administration on page 154
  - Administering the server timer on page 154
  - Administering the Media Gateway on page 155

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 or higher). 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 on page 151
- Call handling during recovery on page 152
- Maintenance during recovery on page 153
- Link recovery unsuccessful on page 153

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 39 lists the timer parameters.

Table 39: 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 40.

Table 40: General Link Recovery process *1 of 2*

Process sequence	Description
1.	Link failure detected (see Conditions that trigger Link Recovery on page 150)
2.	The Primary and Total Search Timers begin running. The gateway attempts to re-establish the H.248 link with original server, which is the first element in the Media Gateway Controller (MGC) list. See Administering the MGC list on page 156 for instructions on administering this list. See Administering the Media Gateway on page 155 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: **S8300**: 1-3 S8300s configured as Local Survivable Processors (LSPs) **S8500** and **S8700 | 8710**: 1-3 C-LAN circuit packs within the primary server's configuration The Total Search Timer continues running. See Administering the MGC list on page 156 for instructions on administering this list and on setting the Transition Point.

1 of 2

Table 40: General Link Recovery process *2 of 2*

Process sequence	Description
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 153 for more information about the server and gateway alarm notification strategies. The server's Link Loss Delay Timer should be the last timer to expire, meaning that the server holds its call control information until all other means of re-establishing the have been exhausted. Note: If the Link Loss Delay Timer expires but the gateway successfully connects with an alternate resource, the system generates a warning alarm anyway, even though the H.248 link is up.

2 of 2

Call handling during recovery

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

- New calls are not processed.
- Calls held in queue for an 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 157 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 41.

Table 41: 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 42.

Table 42: Media Gateway events and alarms *1 of 2*

Event	Alarm level	Log	SNMP
Loss of link	Major	Event	Trap
Link restored	Major	Event	Trap clear
Registration successful	Informational	Event	Trap

1 of 2

Table 42: Media Gateway events and alarms *2 of 2*

Event	Alarm level	Log	SNMP
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

2 of 2

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 a 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 154
- Administering the Media Gateway on page 155
- Administering the MGC list on page 156

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 **IP-Options System Parameters** form (Figure 12).
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 Media Gateway on page 155).
3. Press **Enter** to save the change.

Figure 12: IP-Options System Parameters form

```
change system-parameters ip-options                              Page   1 of   2
                          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: 172.16 .241.80
               Default Server Port: 5005
  Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y


 H.248 MEDIA GATEWAY                  H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5       Link Loss Delay Timer (min): 5
                                         Primary Search Time (sec): 75
                                  Periodic Registration Timer (min): 20
```

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.

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 primary-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 151 for more information about the H.248 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 with the **reset mgp** command.

   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 with the **show mgc** command.

   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 43).

Table 43: H.248 Link Recovery feature/adjunct interactions *1 of 2*

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

1 of 2

Table 43: H.248 Link Recovery feature/adjunct interactions *2 of 2*

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

Network fragmentation

A likely outcome to an H.248 link recovery scenario is that a network of 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. Two methods are available to recover from a fragmented network:

- Auto Fallback to Primary on page 174 describes how this feature reconstructs the server/gateway topology following network fragmentation.
- Execute **`reset system 4`** on each LSP.

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

Shut down Communication Manager on every LSP

The only way to be certain that gateways and endpoints re-register with the primary server is to shut down Communication Manager on every LSP in the network, using the Linux command **`stop -acfn`**. Afterward, the primary server SAT commands **`list media-gateway`** or **`status media-gateway`** can verify whether all the network endpoints re-registered with the primary server. The Linux command **`start -ac`** 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 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 44 provides a synopsis of the recovery outcomes.

Table 44: Synopsis of recovery outcomes *1 of 2*

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.

1 of 2

Table 44: Synopsis of recovery outcomes *2 of 2*

If	Then
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. No new calls are accepted. Features and buttons are inoperable.
	2 of 2

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
- S8300
- S8500
- S8700 | S8710

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

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 45 describes the performance interactions due to link failure-induced time delays.

Table 45: 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, and S8300). 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 13: Idle Traffic Interval on page 164)
- TCP Keep-Alive Interval (see Figure 14: Keep-Alive signals acknowledged by Gateway on page 165)
- Keep-Alive Count (see Figure 15: Keep-Alive signals not acknowledged by Gateway on page 165)

These three (3) administrable parameters are explained in Table 46: Administrable H.323 Link Bounce Recovery parameters on page 166.

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 13.

Figure 13: Idle Traffic Interval

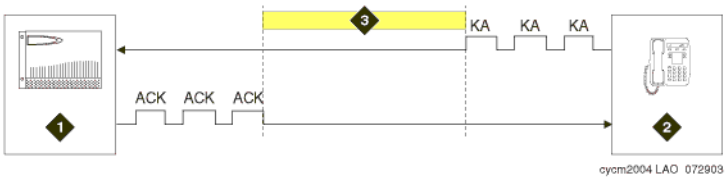


Figure notes:

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

1. Gateway
2. IP endpoint
3. Idle Traffic Interval

The Keep Alive Interval is the time between Keep-Alive messages that the endpoint sends to the Gateway as depicted in Figure 14: Keep-Alive signals acknowledged by Gateway on page 165.

Figure 14: Keep-Alive signals acknowledged by Gateway

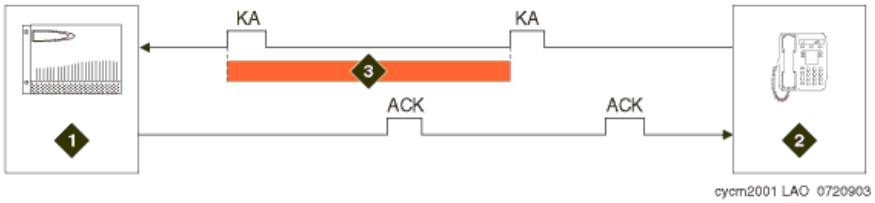


Figure notes:

1. Gateway
2. IP endpoint
3. Keep-Alive Interval

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 15) 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 15).

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 15: Keep-Alive signals not acknowledged by Gateway

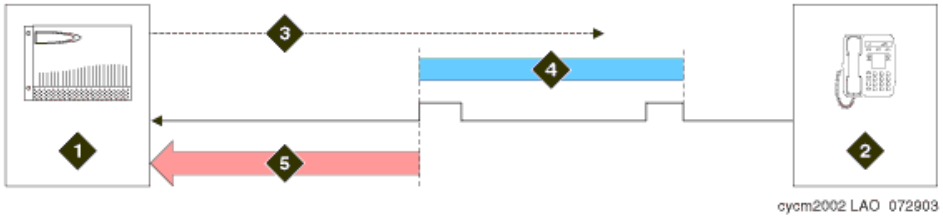


Figure notes:

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

Table 46 lists the administrable parameters that interact within the H.323 Link Bounce Recovery feature. See Administration for how to implement these parameters.

Table 46: 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. **Note:** This timer does not apply to Soft-endpoint telecommuter calls.
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. While off-hook, the endpoint continues trying to re-establish connection with the current server (Gateway) until the call ends.

Link recovery sequence

Table 47 lists the sequence of events during recovery and includes an explanation of what it happening. This sequence correlates with Figure 16: H.323 Link Bounce recovery process on page 169.

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 47: H.323 Link Recovery sequence *1 of 3*

Process sequence	Description
1.	Link failure detected (any of the following): • Gateway detects a TCP socket failure • TCP socket closure • Catastrophic network error on the link • Lack of a TCP Keep-Alive signal from the endpoint (Keep-Alive Count exceeded). See Keep-Alive signals and Note 4 in Figure 15: Keep-Alive signals not acknowledged by Gateway on page 165 for more information.

1 of 3

Table 47: H.323 Link Recovery sequence *2 of 3*

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 16: H.323 Link Bounce recovery process on page 169). • 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. • 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. **Note:** 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 16: H.323 Link Bounce recovery process on page 169) 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 16: H.323 Link Bounce recovery process on page 169) 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 16: H.323 Link Bounce recovery process on page 169).

2 of 3

Table 47: H.323 Link Recovery sequence *3 of 3*

Process sequence	Description
6.	The endpoint continues its re-registration attempts, as depicted by Note 9 in Figure 16: H.323 Link Bounce recovery process on page 169.
7.	When the H.323 Link Loss Delay Timer expires (Note 10 in Figure 16: H.323 Link Bounce recovery process on page 169), the Gateway drops all call state information.
	3 of 3

Use Figure 16: H.323 Link Bounce recovery process on page 169 below to correlate the events in Table 47: H.323 Link Recovery sequence on page 167.

Figure 16: H.323 Link Bounce recovery process

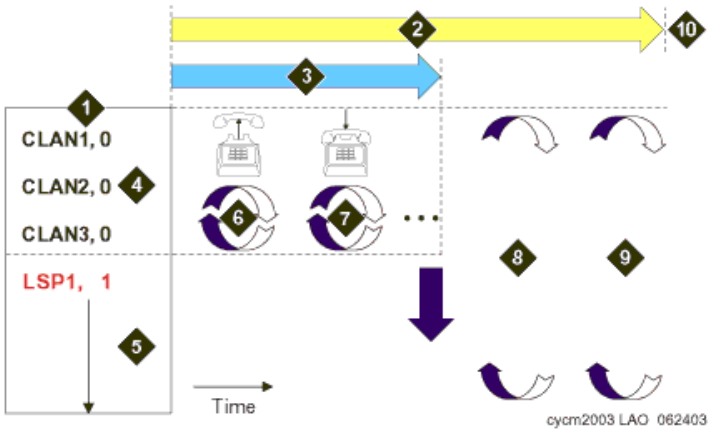


Figure notes:

1. **Alternate Gateway List**
2. **H.323 Link Loss Delay Timer (gateway)**
3. **Primary Search Time (endpoint)**
4. **IP address of alternate C-LAN and Gateway ID**
5. **Local Survivable Processor (LSP) list in search order.**
6. **Endpoint attempts re-registration while call is in progress**
7. **Call ends and endpoint continues re-registration attempts**
8. **Endpoint attempts re-registration to any Gateway in the AGL, including Local Survivable Processors (LSPs)**
9. **Endpoint continues re-registration attempts.**
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 16 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 16: H.323 Link Bounce recovery process on page 169) contains the IP address of a 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 several 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

```
change system-parameters ip-options                              Page   1 of   2
                          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: 172.16 .241.80
               Default Server Port: 5005
  Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y


 H.248 MEDIA GATEWAY                  H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5       Link Loss Delay Timer (min): 5
                                         Primary Search Time (sec): 75
                                  Periodic Registration Timer (min): 20
```

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

Table 48: 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. **Note:** 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 a LSP. While the IP Telephone's receiver is lifted, the endpoint continues trying to re-establish connection with the current server until the call ends.
Periodic Registration Timer	This timer is started when the phone's registration is taken over by another IP endpoint. The timer is cancelled upon successful RAS registration. When the timer expires, the phone tries to re-register with the server. Default timer value: Dependent on the number of unsuccessful periodic registration attempts. As long as the RRJ error message continues to be "Extension in Use," the endpoint continues to attempt registration with the current gatekeeper address. Sample field values apply unless the endpoint is interrupted, such as by power loss, or the user takes manual action to override this automatic process: • **20** means once every 20 minutes for two hours, then once an hour for 24 hours, then once every 24 hours continually. • **60** means once an hour for two hours, then once an hour for 24 hours, then once every 24 hours continually.

IP Network Region

```
                              IP NETWORK REGION
  Region: 1
Location: 1                Home Domain:
    Name:
                                 Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                 Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                             IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3028                        RTCP Reporting Enabled? y
                                RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS          Use Default Server Parameters? y
 Call Control PHB Value: 46
        Audio PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        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 Traffic Interval (sec): 20      Retry upon RSVP Failure Enabled? y
   Keep-Alive Interval (sec): 5                  RSVP Profile: guaranteed-service
            Keep-Alive Count: 5       RSVP unreserved (BBE) PHB Value: 43
```

Table 49: 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. An **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

Auto Fallback to Primary

The intent of this feature is to return a fragmented network, where a number of H.248 Media Gateways (MG) are being serviced by one or more LSPs (Local Survivable Processors), to the primary media server in an automatic fashion. This feature is targeted towards all H.248 media gateways. The main driving force for this feature is the fact that, when an MG is receiving service from a LSP, the notion of the “big single distributed switch” is no longer the case; therefore, resources are not being used efficiently. By migrating the MGs back to the primary automatically, the distributed telephony switch network can be made whole sooner without human intervention, which is required today.

This feature also only addresses “when” an MG shall return to the primary controller, and does not explicitly address how call recovery is attempted during the return. Ideally, the fragmented network should be self-healing, and that process should be transparent to all users whether they are currently on a call or not (in other words, no phones resetting or calls being dropped).

The auto-fallback migration, in combination with the connection preservation feature for H.248 gateways is connection-preserving. Stable connections will be preserved; unstable connections (such as ringing calls) will not be. There still may be a very short interval without dialtone for new calls.

The feature is composed of client and server components, where the client side is the media gateway and the server side is the Avaya Communication Manager (ACM) media server. The client actively attempts to register with the primary server while it maintains its H.248 link to the LSP. This is being done, so that the server can act in a permissive role to allow a registration or deny it. When an MG is being serviced by a LSP, then the Primary Media Server has the option to deny a registration in cases where the media server may be overwhelmed with call processing, or based upon system administration.

The MG presents a new registration parameter in the Non-Standard Data that indicates that Service is being obtained from a LSP, and indicates the number of calls currently active on the MG platform (number of active user calls). The server administers each MG to have its own set of rules for Time of Day migration, enable/disable, and the setting of context threshold rules for migration.

This feature allows the administrator to define any of the following rules for migration:

- The MG should migrate to the primary automatically, or not.
- The MG should migrate immediately when possible, regardless of active call count.
- The MG should only migrate if the active call count is 0.
- The MG should only be allowed to migrate within a window of opportunity, by providing day of the week and time intervals per day.

  This option does not take call count into consideration.
- The MG should be migrated within a window of opportunity by providing day of the week and time of day, *or immediately* if the call count reaches 0.

  Both rules are active at the same time.
- The **Minimum Time of Network Stability** field (see Communication Manager administration for manual configuration on page 208) is administrable to fit the recovery strategy.

Internally, the primary call controller gives priority to registration requests from those MGs that are currently not being serviced by a LSP. This priority is not administrable.

A more detailed discussion and administrative procedures for Auto Fallback to Primary are in *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504*.

Local Survivable Processor (LSP)

The S8300 and S8500 (through the Processor Ethernet interface) Media Servers can act as a survivable call-processing servers for remote or branch customer locations. As LSPs, they have a complete set of Communication Manager features, and its license file allows it to function as a survivable call processor. If the link between the media gateways and the primary controller is broken, those telephones and gateways that are designated to receive backup service register with the LSP. The LSP provides control to those registered devices in a license error mode (see *Hardware Description and Reference for Avaya Communication Manager, 555-245-207*).

Returning an active LSP to standby mode

When the primary media server is available again, it begins handling calls, however, for configurations earlier than Release 3.0 (Auto Fallback to Primary feature returns active LSPs to standby mode) endpoints that were registered with the LSP stay registered it until the LSP is rebooted.

CAUTION:

This procedure reboots the LSP, dropping all calls. Ensure that you perform this procedure from the LSP, *not the active server*.

To return an active LSP to standby mode:

1. At the Maintenance Web Interface *for the LSP* in the Sever section select **Shutdown Server**.

   The **Shutdown Server** page displays.

2. Select **Delayed Shutdown**.

   WARNING:

   Shutting down this server also stops the Web server that you are currently communicating with, so you will be unable to access these Web pages until the system starts again.

3. Check the "Restart server after shutdown" box.
4. Click on the **Shutdown** button.
5. Verify that all media gateways have re-registered with the main server.
6. Log back on to the LSP through SAT interface for the LSP.
7. Type **`status media-gateway`** to display the **Media Gateways** page.
8. In the H.248 LINK SUMMARY section, the **Links Up** field should read **0**.

   In the Alarms section the **Lk** column should read **dn** for all gateways.

Enterprise Survivable Server (ESS)

In the media gateway architecture today, media gateways register with a primary call controller; however, the IP interface through which the media gateway registers can either be on the call controller directly in the case of the S8300 Media Server, or through a C-LAN interface in the case where the call controller is an S8700 Series or S8500 Series Media Servers (through the Processor Ethernet interface).

The Enterprise Survivable Servers (ESS) feature provides survivability to Port Networks by allowing backup servers to be placed in various locations in the customer’s network. The backup servers supply service to Port Networks in the case where the S8500-series media server, or the S8700-series media server pair fails, or connectivity to the main Communication

Manager server(s) is lost. ESS servers can be either S8500-series or S8700-series media servers, and offer full Avaya Communication Manager functionality when in survivable mode, provided sufficient connectivity exists to other Avaya components (for example, endpoints, gateways, and messaging servers). One exception is that an ESS cannot control a Center Stage Switch.

When designing a network to support ESS servers, consider the following:

- ESS servers can only control Port Networks that they can reach over an IP network. That is, ESS servers connected on an enterprise's public IP network will not be able to control Port Networks connected to Control Network A or B, unless:
  - ESS can control a remote Port Network that is connected through ATM or Center Stage to Port Networks on Control Networks A or B, or
  - Control Networks A or B are exposed to the public IP network through Control Network on the Customer's LAN (CNOCL).
- Multiple ESSs can be deployed in a network. In the case above, an enterprise could deploy one or more ESSs on the public network, and an additional server on Control Networks A and B to backup Port Networks attached to the respective networks.

  However, when Port Networks register with different ESS servers, system fragmentation may occur. In that case, care should be taken to establish adequate trunking and routing patterns to allow users at a particular location to be able to place calls where needed.
- ESS servers register to the main server(s) through a C-LAN. Each ESS must be able to communicate with a C-LAN in order to download translations.

The media gateway cannot distinguish between registration through a C-LAN or registration to a media server directly. Prior to Communication Manager 3.0, without ESS, if a media gateway successfully registered with a primary call controller IP address, then the media gateway was properly registered with the primary call controller. However, in Communication Manager 3.0 and later, when a media gateway completes a successful registration through an IP address defined as a primary call controller address, if that address is a C-LAN, the media gateway may not necessarily be registered with the true primary call controller. The port network that houses the C-LAN may be under control of an ESS; but the media gateway will not know that it is registered with an ESS.

When the traditional port network migrates back to the primary call controller, then the media gateway loses its H.248 link, and the Link Loss Recovery algorithm engages, and that should be sufficient. The Auto Fallback to Primary feature only engages if the media gateway drops the connection and registers with an LSP. The ESS migration should only occur if the port network is reasonably certain to return to the primary call controller, so the media gateway would simply return to the same C-LAN interface. Now, when the media gateway returns to the same C-LAN interface, the Link Loss Recovery feature performs a context audit with the primary controller and learns that the primary call controller is not aware of the media gateway. The controller in this case issues a warm start request to the media gateway, or potentially different behavior if connection preservation is active at the same time. The Auto-Fallback feature is not affected by ESS.

For more information on ESS, see the *Using the Avaya Enterprise Survivable Servers (ESS), 03-300428*.

Standard Local Survivability (SLS)

Standard Local Survivability (SLS) provides a local G250 Media Gateway with a limited subset of Communication Manager functionality when there is no IP-routed WAN link available to the main server or the main server is unavailable.

SLS provides

- Calling capability among analog, DCP, and IP phones
- Outbound dialing through the local PSTN (local trunk gateway) from analog, DCP, and IP phones
- Inbound calls from each trunk to pre-configured local analog or IP phones that have registered
- Direct Inward Dialing (SLS)
- Multiple call appearances
- Hold (SLS) and Call Transfer (SLS) functions
- Contact closure feature
- Local call progress tones (dial tone, busy, etc.)
- Emergency Transfer in survivable mode on the media gateway hardware in cases of power loss
- Auto Fallback to Primary Server
- IP station registration
- SLS supports the Avaya phones listed in Table 50

Table 50: Avaya phones supported in SLS, *1 of 2*

Analog	DCP	IP
2500	2402	4601
	2410	4602
	2420	4602sw
	6402	4610sw
	6402D	4612
	6408 (default)	4620
	6408+	4620sw
		1 of 2

Table 50: Avaya phones supported in SLS, *2 of 2*

Analog	DCP	IP
	6408D	4621
	6408D+	4622
	6416D+	4624
	6424D+	4625
	8403B	
	8405B	
	8405B+	
	8405D	
	8405D+	
	8410B	
	8410D	
	8411B	
	8411D	
	8434D	
		2 of 2

Prerequisites

- Communication Manager Release 3.1 or later running on the host server
- PIM or configuration of the G250 through its CLI
- Registration of the G250 with Communication Manager
- SLS enabled on the G250 through its CLI
- No access to Communication Manager on the S8500 through the Processor Ethernet interface
- S8300 is not serving as a LSP
- G250 is not subtending to another external server (including ESS or another LSP in another gateway).

Licensing

SLS is part of the basic offering and does not require a separate license.

Detailed description

Because small gateways can be widely distributed throughout a customers' network, service interruptions somewhere in the WAN are also likely, increasing the chances that a media gateway has no call controller available to it. Standard Local Survivability (SLS) on the Avaya G250 Media Gateway provides basic telephony service in the absence of a main Communication Manager controller (server, LSP).

As one of the most affordable offers in Avaya's recovery strategy, SLS is not a replacement for Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP) survivability which offer full call-feature functionality and full translations in the survivable mode. Instead, SLS is a cost-effective survivability alternative offering Limited call processing in survivable mode and no special station features. Although the G250 has an option to host S8300B servers as an ICC or LSP and S8500B through the Processor Ethernet interface, SLS offers both local survivability and call control.

In contrast to the server-based survivability features, SLS operates entirely from the media gateway and requires a data set (see Complete provisioning data on page 182) comprised of:

- Communication Manager translations (Survivable ARS Analysis and configuration data)
- Provisioning and Installation Manager (PIM) tool that can distribute bulk provisioning to a group of similar devices.

  -or-

- A manually-configured SLS data set that is administered at the command line interface (CLI) on the G250 Media Gateway (in the absence of PIM)

Ideally, the PIM gathers data from Communication Manager that are sent to the G250 gateway and stored in non-volatile RAM (NVRAM), waiting for activation. If PIM cannot build the SLS data set and deliver it to the media gateway, then the data set can be created manually through the media gateway command-line interface (CLI, see Manually configuring the SLS data on the media gateway on page 208).

Once the SLS data set is in place and the gateway is ready to provide SLS service, How the G250 enters survivable mode on page 185 discusses the events surrounding the loss of the H.248 signaling link between the server and the gateway and how and when SLS is launched.

Limited call processing in survivable mode

In survivable mode, SLS provides only a limited subset of Communication Manager call processing functionality:

- Limited call routing through a Survivable ARS Analysis Table (in the PIM application or through the CLI) and COR calling permissions.
- Inbound calls are directed to a previously-administered pool of available stations (the **Survivable Trunk Dest?** field is y on the **Station** form). The search algorithm is circular so that the incoming calls are fairly distributed.

  Important:

  SLS permits 911 calls, but the specific location information is not transmitted to the Public Service Answering Point (PSAP) but only the general trunk-identifying information. Emergency personnel will have a general location associated with the trunk (for example, a building address), but nothing more specific like the room or office number. Also, If a 911 call disconnects for any reason, emergency personnel cannot reliably call the originator back.
- Communication Manager Feature Access Codes for ARS, Contact Closure, and Hold
- Acts as H.323 Gatekeeper that allows IP endpoints to register simultaneously
- Direct Inward Dialing (SLS)
- Multiple call appearances
- Hold (SLS) and Call Transfer (SLS) functions
- Contact closure feature
- Call Detail Recording (CDR, see SLS logging activities on page 198)
- Trunk Access Code (TAC) dialing
- Centrex features

  Note:

  SLS cannot add or delete digits for outbound calls to the analog loop-start (CO) trunk. This means that Centrex users, for example, must manually dial the extra digit(s) before they can call out to the PSTN. If the CO access code is "9," then a Centrex customer would have to dial "9-555-1212" for local directory service. If this Centrex access code is not dialed correctly, the local outbound PSTN call will not complete successfully.

SLS does not support the following functionality in Release 3.1:

- Many small business customers employ custom calling features like call waiting from the BOC/LEC, attempting a more PBX-like capability. These features are not supported by SLS.
- ISDN BRI trunks

- E1/T1-PRI trunks
- T1 In-band signaling on trunks
- E1 In-band signaling on trunks
- ‘Calling party name/number’ information to digital station displays
- Caller ID on outgoing analog station calls
- Caller ID on incoming analog loop-start trunk calls
- 3-party conferences
- Last Number Redial
- Call Forwarding-Busy/Don’t Answer
- No Music On Hold source or announcement playback
- Call Center features, including ASAI
- Connection Preserving Failover/Failback for H.248 Gateways

Complete provisioning data

SLS requires that the G250 Media Gateway has connected to a Communication Manager server at least once and has received provisioning information, which includes:

- Communication Manager port information through the H.248 control channel
  - Tone sources, including a distinctly different dial tone to inform users that the system is operating in survivable mode
  - Loss plan
- Communication Manager analog resource information through the CCMS channel
- Provisioning and Installation Manager (PIM) queries Communication Manager for station/trunk configuration and dialplan routing administration data through SNMP.

These data sources and communication links are described in Figure 17.

Figure 17: G250 Standard Local Survivability data sources and communication paths

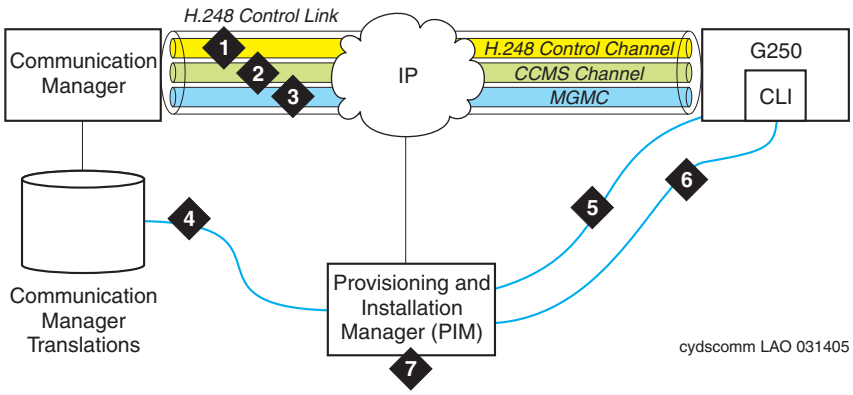


Figure notes:

1. **H.248 call signalling and configuration data**
2. **CCMS messages through Clear Channel**
3. **Media Gateway Maintenance Channel**
4. **PIM extracts Communication Manager translation subset through OSSI**

   NOTE: You do not have to configure the PIM, but the SLS data must be configured manually in the gateway if the PIM is not available.
5. **PIM data set and SLS MIB delivered to G250 through SNMP**
6. **Security codes (passwords) sent over SSH connection to CLI**
7. **Provisioning and Installation Manager (PIM) for remotely provisioning gateways, network-wide. PIM is installed on an enterprise management server, not on the primary Communication Manager server.**

The required Communication Manager translations for SLS include new fields on the **Station** and **Media Gateway** forms. See Communication Manager administration on page 200 for more information about the information types and how to administer Communication Manager for SLS.

SLS also requires PIM configuration data, some of which it extracts from the Communication Manager translations. PIM aggregates the required data and over a secure communication path copies the provisioning data to non-volatile RAM (NVRAM) on the media gateway. After the initial data collection, PIM retains a copy of the data set for each media gateway. This set is compared with subsequent data sets to determine if anything has changed:

- If the data set changes, then the newer data set is pushed down to the media gateway.
- If the data set does not change, then the data set in NVRAM remains unchanged.

Users can schedule when to collect and push data, perform scheduled/manual backups, enable/disable SLS, as well as display (but not change) the data to ensure correct information.

If PIM is unavailable, the SLS data set can be manually configured (see Manually configuring the SLS data on the media gateway on page 208).

Communication Manager data

Two Communication Manager forms are part of the provisioning data necessary for SLS (see Communication Manager administration on page 200 for details):

- **Station** form (**`add station`**)
  - **Survivable COR** field places a restriction level for stations to limit certain users to only certain types of calls. (values = **emergency**, **internal**, **local**, **toll**, and **unrestricted**). See Figure 24: Inherited Class of Restriction (COR) permissions on page 211 for more information about the inherited COR hierarchy.
  - **Survivable Trunk Dest?** (**y**/**n**, default is **y**) field allows stations to receive incoming trunk calls or not in the survivable mode.
- **Media Gateway** form (**`add media-gateway next`**): **Max Survivable IP Ext** field only appears when the **Type** field is **G250**. The limited VOIP resources in SLS can only handle so many simultaneous IP endpoint registrations, and this field limits that number.

  Important:
  Since the VOIP resources on the G250 Media Gateway are limited, the **Max Survivable IP Ext** field should not be set larger than 12.

The primary server's translations are the source of the information that the PIM application gathers and pushes down to the media gateway. Although a server functioning as an ESS or LSP should have the same translations as the primary, the ESS/LSP translations can be altered (but not saved), making the primary server's translations the best data to send to the media gateway. If for diagnostic reasons you want to change any parameter that PIM pushes to the media gateway, you can change the SLS data set through the CLI on the media gateway.

PIM data

Three forms within the PIM application must be administered for SLS to work properly:

- **Add ARS Dial String form** to administer an Automatic Route Selection
- **Survivability form** to view a summary report of the strings entered
- **Survivable ARS Analysis Table** provides local PSTN access based on the call routing that is administered on this form. Data from this form provide the survivable dial plan for analyzing dial patterns and routing the calls according to the local dial plan.

See NMC and PIM administration on page 202) for examples of the required PIM administration.

How the G250 enters survivable mode

Gateway loses signaling to server

Figure 10: Recovery timers and their interactions on page 137 shows the loss of the H.248 signaling link between the server and the gateway (including loss of the server-to-IPSI Ethernet link), interactions among Avaya's recovery processes, and describes the associated timers.

Note:

During the transition to survivability mode, only shuffled (local IP-to-IP) calls are preserved; all others are dropped.

Media Gateway Controller list

A new element that displays in the Media Gateway Controller (MGC) list called the "survivable-call-engine" is the last element in the list and always past the Transition Point (Note 7 in Figure 10: Recovery timers and their interactions on page 137). After the Link Recovery search concludes for the primary controller list (entries above the Transition Point), it then searches the alternate controller list (entries below the Transition Point), ending with "survivable-call-engine," the last-choice call controller for the gateway.

The media gateway loops through the primary controller list in order for the duration of the Primary Search Timer (PST, Note 4 in Figure 10: Recovery timers and their interactions on page 137), crosses the Transition Point (Note 7 in Figure 10: Recovery timers and their interactions on page 137), then proceeds down the list of alternate controllers in order for the duration of the Total Search Timer (TST, Note 3 in Figure 10: Recovery timers and their interactions on page 137). If none of the connection attempts with first four elements of MGC list are successful, then survivable-call-engine is invoked, activating SLS in the media gateway. If "survivable-call-engine" is the only entry in the list, then SLS is invoked if it has been properly provisioned (see Complete provisioning data on page 182). Since SLS is a potential alternate controller, it answers the registration request after the last entry in the MGC list has been tried and rejected. You cannot administer the SLS IP address in the first four entries of the MGC list; "survivable-call-engine" can only be the fifth entry.

While in survivability mode and before the recovery timers expire, the media gateway continues trying to register with a Communication Manager server in the MGC list. Any call-controller (server) is preferred over SLS, but if all of the MGC elements are exhausted, then SLS is the media gateway's final recovery option.

SLS states

When the Link Recovery search settles on the "survivable-call-engine" entry in the MGC list, then the G250 registers with SLS (resident on the media gateway) for its call control. This section discusses each of the four possible SLS states and the transitions from one state to another.

Unregistered

This is the "normal" state in which SLS waits for an H.248 registration request from the media gateway. When SLS receives the request, it registers the gateway and transitions to the Setup state.

Setup

In this transitional state SLS performs the following activities:

1. Checks for proper provisioning data (see Complete provisioning data on page 182). If there is insufficient provisioning, then the registration request is denied, and SLS returns to the Unregistered state.
2. Initializes SLS components such as gatekeeper data (for example, IP endpoint's E.164 addresses and passwords), dial plan, and ARS routing.
3. Completes H.248 registration with SLS.
4. Creates the H.323 GateKeeper socket after successful registration.

When Setup is complete, SLS transitions to the Registered state.

Registered

SLS can only process calls while it is in the Registered state in which it:

1. Constructs endpoint objects based on board insertion and IP registration
2. Tears down endpoint objects based on board removal and IP unregistration
3. Handles registration requests from H.323 endpoints that display the IP address that has been discovered (the media gateway's IP address) or searching for.
4. Handles stimuli from all interfaces

SLS remains in the Registered state as long as the socket to SLS is open.

Teardown

SLS transitions to the Teardown state whenever:

- A Technician invokes the set survivable-call-engine disable command from the CLI.

  -or-

- The media gateway closes the SLS socket after maintenance determines that it has completed an H.248 registration with the Communication Manager server.
- SLS determines that it needs to unregister with the media gateway due to internal error conditions.

In this transitional state SLS:

1. Tears down endpoint objects
2. Sends unregistrations requests to IP endpoints that are not on active calls. IP endpoints lose registration with SLS and display the discovered IP address during re-registration with a Communication Manager server.
3. Closes the H.323 GateKeeper socket

After Teardown has completed, SLS transitions to the Unregistered state.

Direct Inward Dialing (SLS)

Direct-Inward-Dial (DID) is a service offered by telephone companies that enables callers to dial directly into an extension on a PBX without the assistance of an operator or automated call attendant.

Note:

DID is a method of routing calls that applies to both analog and digital (T1/E1) lines. However, while the method is typically referred to as DID in the analog world, it is usually called Dialed Number Identification Service (DNIS) in the digital world. Despite the difference in names, the concept is the same.

The G250 gateway supports a maximum of 2 analog DID central office trunk interfaces, and the digit transmission from the central office is configurable when ordering the service:

- **Immediate** - the DID signaling starts immediately after the central office seizes the loop-start trunk. In addition, analog DID trunk lines only support inbound calls. For that reason, CPE utilizing DID trunk lines for inbound routing would utilize loop-start (for example) lines for outbound transmission.
- **Wink** - the DID signaling starts after the phone reverses battery polarity and sends the "wink" to the central office.

WARNING:

An analog 2-wire DID trunk line is different from a standard analog loop-start line. With analog DID trunk lines, the battery (power feed) to the line is supplied by the phone system. With a standard loop-start line the power is supplied by the central office, and this is why damage can occur from connecting a loop-start line to the DID port.

The number of sent digits (3-4 typically) and signaling type (Pulse/DTMF) are also configurable at ordering time.

Multiple call appearances

When a G250 gateway is in SLS mode, 3 call appearances, each with limitations, are supported:

- The first 2 call appearances are for incoming or outgoing calls. The first call appearance is the default.
- The third call appearance is for outgoing calls only.

Note:

"First," "second," and "third," refer to the order in which you use call appearances, not the order of the call appearance buttons on your phone.

For example, if User A chooses the third call appearance to dial User B the User C calls User A, which is sent to the first call appearance. In this situation a subsequent inbound call to User A will be denied (busy) because the first and third call appearances are in use, and the second call appearance is only available for outbound calls.

Hold (SLS)

Using the Hold feature differs by user and by phone type, and the same is true of the Hold feature in Standard Local Survivability (SLS) mode. Some users return to a call on Hold by pressing the call appearance button, however Communication Manager has an administrable parameter that allows users to release a call on hold by pressing the Hold button a second time (if only one call is held). The Hold feature also works differently in DCP and IP phones and Analog phones in the survivable mode.

The Hold feature in SLS does not support:

- Music on Hold
- Local mute on analog phones
- Specialized treatment of E-911 calls
- Call Hold indicator tones

DCP and IP phones

When a media gateway is in the survivable mode, you can release calls on Hold on all DCP and IP phones by either

- Pressing the Hold button a second time (if only one call is held)
- Pressing the winking call appearance button

Note:

The SLS Hold feature does not support "hard" Hold on DCP and IP phones.

Analog phones

Newer analog phones (for example, Avaya 62xx series) have buttons with specific functions for placing a call on Hold:

- Hold button sends the hold message to the server (see Using the Hold button)
- Flash button sends switchhook signal to the server (see Using the Flash button)
- Switchhook (receiver on/off hook) sends disconnect signal to the server (see Using the switchhook)

Using the Hold button - To place an established call on Hold using the Hold button:

1. Press the Hold button on the analog phone.
2. To return to the call, press the Hold button.

Using the Flash button - To place an established call on Hold using the Flash button:

1. Press the Flash button on the analog phone.

   You will hear dial tone; the other party hears silence.

   You can leave the call on Hold or transfer the call. Press the Flash button twice to return to the call.
2. Dial the Feature Access Code for Hold.

   At this point you can leave the call on Hold or transfer the call.
3. To return to the call, press the Flash button again.

   The call is re-established.

   Note:

   Either party can put the call on Hold or return to the call.

Using the switchhook - To place an established call on Hold by flashing the switchhook:

1. Press the switchhook once.

   You will hear dial tone.

2. Dial the Feature Access Code (FAC) for Hold.

   This places the call on Hard Hold which prevents you from transferring the call. To return to the call, dial the FAC for Hold.

3. You can do any of the following:

   a. Return to the call by dialing the FAC for Hold.

      The call is re-established.

   b. Hang up.

      Your phone will ring to notify you that you have a call on Hold. When you lift the receiver you will hear dial tone and can perform any of the activities listed in Step 3.

   c. Dial a third party by dialing the number and flashing the switchhook once (you will hear stutter dial tone). Dial the FAC for Hold (the second call is now on Hold and the first call is re-established). If you want to toggle between the first and second calls, press the switchhook and dial the FAC once each time you want to change calls.

Call Transfer (SLS)

Using the Call Transfer feature differs by user and by phone type, and the same is true of the Hold feature in Standard Local Survivability (SLS) mode. Call Transfer also works differently in DCP/IP phones and analog phones in the survivable mode.

Call Transfer in SLS:

- Requires that the established call is initiated from a local G250 station or from an incoming trunk. You can make only point-to-point call transfers to a phone that is local to the G250 gateway.
- Does not support E-911 calls
- Does not support the Conference button on any phone
- Does not support trunk-to-trunk transfer (for example, for voice messaging)

DCP and IP phones

To transfer a call on DCP and IP phones in Standard Local Survivability (SLS) mode:

1. While talking on a call or while you have a call on Hold, press the **Transfer** button on your phone.

   You will hear dialtone; the other party hears silence.

2. Dial the third party's number on your phone.
3. You can either
   - Wait for the third party to answer and announce the call and either press the **Transfer** button again or hang up.
   - Transfer the call before the third party answers by pressing the **Transfer** button again.

   The person you were talking to is transferred to the third party.

   Note:

   If you do not completely dial the string or if you hear a fast-busy or re-order (French siren) tone, only a Hard Hold call connection (if present) remains at the station.

   If the third party does not answer, the call does not ring back to the originating party. If a transfer does not complete, the event is logged.

Analog phones

Newer analog phones (for example, Avaya 62xx series) have buttons with specific functions for transferring a call:

- Switchhook (receiver on/off hook) that sends a disconnect signal to the server
- Transfer/Flash button that sends a transfer message to the server

To transfer an established call from an analog phone:

1. While on a call, press the switchhook once or press the **Transfer/Flash** button.

   You will hear dial tone; the other party will hear silence.
2. Dial the third party's number on your phone.
3. You can either
   - Wait for the third party to answer and announce the call, then hang up.
   - Transfer the call before the third party answers by hanging up.

   The person you were talking to is transferred to the third party.

   A message appears on your phone display to indicate that the call transfer was completed. If the necessary call processing resources are not available, the transfer does not complete and the event is logged.

   Note:

   Displays are not supported on analog phones unless they are supported locally by an analog phone.

Contact closure

The Contact Closure feature allows a user to trip a relay that can activate a door opener, an external alarm relay, analog recording system, or anything with a simple on/off relay function by dialing the phone. Topics in the section include:

- Administering Contact Closure on page 192
  - Contact Closure, Communication Manager administration on page 192
  - Contact Closure, G250 gateway administration on page 194
- Using Contact Closure in SLS mode on page 194
- Contact Closure / SLS feature interactions on page 195

Contact Closure is available on these gateways:

- G350 (Release 2.0)
- G250 (Release 3.0)

The Contact Closure feature is a controllable relay providing dry contacts for various applications. To implement the Contact Closure feature, an Avaya Partner Contact Closure Adjunct box is connected to the CCA port on the G250 front panel using a standard telephone cable with RJ-11 connectors at each end.

You can activate, deactivate, or pulse electrical devices using Contact Closure from a phone by dialing a Feature Access Code (FAC) while in SLS mode. You can also activate and deactivate Contact Closure using CLI commands at the G250 Media Gateway.

Administering Contact Closure

You can initiate Contact Closure from your phone or from the gateway CLI:

- If you want to use the phone to implement Contact Closure, use the information in either Contact Closure, Communication Manager administration on page 192 or Contact Closure, G250 gateway administration on page 194.
- If you want to initiate Contact Closure solely from the gateway CLI, use the information in Contact Closure, G250 gateway administration on page 194.

Contact Closure, Communication Manager administration - When administering the server for Contact Closure, these options apply:

- The ‘open’ and ‘close’ FACs must be administered as a pair.
- The ‘pulse’ FAC can be administered independently.

To administer Contact Closure in Communication Manager:

1. At the SAT type **change feature-access-codes** and press **Enter** to display the Feature Access Code (FAC) form.

Feature Access Code (FAC) form

```
change feature-access-codes                                    Page 1 of x
                                FEATURE ACCESS CODE (FAC)
            Abbreviated Dialing List1 Access Code: ____
            Abbreviated Dialing List2 Access Code: ____
            Abbreviated Dialing List3 Access Code: ____
   Abbreviated Dial - Prgm Group List Access Code: ____
                        Announcement Access Code: ____
                         Answer Back Access Code: ____
                           Attendant Access Code: ____
         Auto Alternate Routing (AAR) Access Code: ____
          Auto Route Selection (ARS) Access Code1: ____  Access Code 2: ____
                    Automatic Callback Activation: ____   Deactivation: ____
   Call Forwarding Activation Busy/DA: ____   All: ____   Deactivation: ____
                           Call Park Access Code: ____
                         Call Pickup Access Code: ____
   CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                     CDR Account Code Access Code: ____
                           Change COR Access Code: ____
                      Change Coverage Access Code: ____
                        Contact Closure Open Code: ____     Close Code: ____
                       Contact Closure Pulse Code: ____
```

2. Type the Feature Access Code for any of these three fields:
   - **Contact Closure Open Code**
   - **Close Code**
   - **Contact Closure Pulse Code**

   Note:

   When using rotary-dial analog phones that do not have "*" and "#," do not administer FACs with these characters.

3. Press **Enter** to save the changes.

Contact Closure Open Code - same as the dialplan's Feature Access Code to open a Contact Closure relay. This field must be administered if the **Contact Closure Close Code** field is administered.

Close Code - same as the dialplan's Feature Access Code to close a Contact Closure relay. This field must be administered if the **Contact Closure Open Code** field is administered.

Contact Closure Pulse Code - same as the dialplan's Feature Access Code to pulse a Contact Closure relay.

Contact Closure, G250 gateway administration - To administer the G250 Media Gateway for Contact Closure by dialing a Feature Access Code:

1. At the gateway CLI type **set contact-closure admin *module/port:relay mgc*** to set the Contact Closure on the Gateway. For example the following command permits your dialing a Feature Access Code to activate/deactivate Contact Closure:

   set contact-closure admin *10/1:1 mgc*

   sets module 10, port 1, relay 1 under control of the MGC list.

2. At the gateway CLI type **set contact-closure pulse-duration *module/port:relay*** to set the length of time that the Contact Closure pulses, for example:

   set contact-closure pulse-duration *10/1:2 5*

   pulses module 10, port 1, relay 2 for 5 seconds.

3. To activate or deactivate Contact Closure manually:

   - At the gateway CLI type **set contact-closure admin *module/port:relay manual-trigger*** to activate Contact Closure, for example:

     set contact closure admin *10/1:1 manual-trigger*

     closes the contacts on module 10, port 1, relay 1.

   - At the gateway CLI type **set contact-closure admin *module/port:relay manual-off*** to deactivate Contact Closure, for example:

     set contact closure admin *10/1:1 manual-off*

     opens the contacts on module 10, port 1, relay 1.

Using Contact Closure in SLS mode

When the media gateway is in survivable mode, Contact Closure works as follows:

1. Lift the phone receiver and listen for survivability dialtone.
2. Dial the appropriate Contact Closure FAC (open, close, or pulse) on the phone.
   - If you dial an invalid FAC code, then SLS plays an intercept tone and terminates the session.
   - If you dial a valid FAC code, then you will hear standard dial tone and can proceed to Step 3.
3. Dial the media gateway number (3 digits).
   - If you enter fewer than 3 digits, then SLS times out and you must restart this procedure from the beginning.
   - If media gateway number matches the local media gateway number, then SLS plays standard dialtone and you can proceed to Step 4.
   - If the media gateway number does not match the local media gateway number, SLS plays an intercept tone and terminates the session.

4. Dial the Contact Closure code, for example "1" for contact closure 1, "2" for contact closure 2.

   You will hear stutter tone and then silence confirming these valid codes. If you dial an invalid Contact Closure number, you will hear an intercept tone.

   - Dialing errors are logged in the Media Gateway error log.
   - Contact Closure feature activations appear in the CDR log (see Figure 19: CDR log example, Contact Closure on page 199).

Contact Closure / SLS feature interactions

- There is no screening to authorize Contact Closure feature use in SLS mode. Security is provided by limiting the number of users who know the correct key sequence required for the Contact Closure feature.
- You cannot use the Hold or Transfer features while dialing the Contact Closure FAC key sequence.
- Contact Closure will not work until you dial the full digit sequence and it is processed.
- If two users try to simultaneously use Contact Closure, whoever dials the full FAC key sequence first gets precedence.
- Interdigit timing rules apply to the Contact Closure feature, so that if you pause too long during the FAC key sequence, the feature times out.
- Call appearances are not released (available for calls) until you hang up.
- You cannot use the Contact Closure feature from outside trunk lines.

IP Softphone shared administrative identity

The SLS mode supports shared administrative identity with the Avaya Softphone application, but requires specific station administration:

1. At the SAT type **`change station`** ***`extension`*** and press **Enter** to display the **Station** form.
2. Set the **Terminal Type** field to a 46xx IP phone.
3. Save the changes.

Note:

If you administer the **Terminal Type** field as a DCP phone, shared administrative identity functionality in SLS mode is not supported.

Gateway translation conversion

In order to re-use a Release 3.0 CLI translation file you must convert it to the Release 3.1 command syntax.

To convert a Release 3.0 CLI translation file to the Release 3.1 formats:

1. At the CLI prompt type **`copy ftp running-config`** and press **Enter** to save the Release 3.0 CLI translation file to the G250 gateway.
2. Reset the G250 gateway.
3. At the CLI prompt type **`copy running-config start-up-config`** and press **Enter**.

   A gateway application reconstructs the CLI commands to use the Release 3.1 command contexts and subcommand formats and saves the results in a new translation file.

Preventing PIM updates

Avaya recommends that you turn off automatic PIM updates while you are manually administering or troubleshooting the G250 Media Gateway.

Note:

You must be in the survivable context before you can issue any of the commands in this section.

To turn off PIM updates:

1. At the command line interface type **`set pim-lockout y`** and press **Enter**.

To re-instate the PIM updates:

1. At the command line interface type **`set pim-lockout n`** and press **Enter**.

If you want to look up the PIM update status:

1. At the command line interface type **`show pim-lockout`** and press **Enter**.

   PIM Lockout = yes/no displays.

Emergency Transfer in survivable mode

Emergency Transfer Relay (ETR) on the G250 Media Gateway connects or "latches" an analog loop-start CO trunk port to an analog station port, allowing the user to access the PSTN for emergency calls in these conditions:

- Power outage
- Loss of controller, including SLS, dropping calls on either the trunk port or the station port. Once the gateway registers with SLS, ETR unlatches.
- CLI command can set ETR to
  - **auto**, meaning that the ETR ports are connected if no controller is active.
  - **on**, meaning that the connection is always present.
  - **off**, meaning that the connection is never made. However, if there was a connection and ETR is set to off, the call stays up until it is disconnected, normally making the ETR ports available.

The Emergency Transfer for each of the gateway models closes the tip/ring contacts for the ports listed in Table 1.

Table 1: Emergency Transfer trunk-to-port latching

G250 model	Analog loop start trunks	Analog station ports
G250-Analog	V301	V305[1]
G250-BRI	V301	V302
G250-DCP	V301	V305
G250-DS1	V301	V302

1. These values are permitted only if they are not previously administered as DID trunks.

If SLS is disabled, then the ETR remains latched unless the media gateway registers with a Communication Manager server or the state is changed through a CLI command or SNMP. There can only be one ETR call, so upon registering with a server, the gateway ports are polled to determine an ETR call is active. If there are none, the ETR disengages, and the ports are returned to normal service. Otherwise, the gateway remains in Emergency Transfer mode until the ports are idle. If the gateway is still in ET mode after the gateway registers with a new server, Communication Manager maintenance must busy out the ports until it receives notification that the ports are idle and available for use.

You can busy out the ports from the SAT either before or after Emergency Transfer mode is invoked, but you might get abort codes depending on the circumstances:

- If you issue the **busyout board** or **busyout port** command and
  - the ports are idle, then the system busys out the ports.
  - the ports are in use, then the system returns an Abort Code 1010, "port already busy."
- If you issue the **release board** or **release port** command, but the gateway has control of these ports while it is in Emergency Transfer mode, the system returns Abort Code 1426, "cannot release ports, MG has control."

You cannot disable the ETR feature when the G250 gateway is powered down.

CAUTION:

Some ports should not be administered as DID ports to avoid having the ETR “loop-start” trunk connected directly to the tip and ring circuit of the DID trunk, thus creating two battery feed circuits driving one another.

For the following models *do not* use the indicated Integrated ports for DID:

- G250: Integrated port V305
- G250-BRI: Integrated port V302
- G250-DCP: Integrated port V305
- G250-DS1: Integrated port V302

SLS logging activities

SLS exports call-recording data in survivability mode. The **Call Detail Record (CDR) log** contains detailed information about each outgoing call that uses a trunk. This information can be stored in flash NVRAM or directed to an external server for later processing and includes data for:

- Merged outgoing Trunk Access Codes (TACs), indicating successfully completed dialing
- Successfully completed ARS calls, as shown in Figure 18: CDR log example, successful ARS calls on page 199
- Contact Closure, as shown in Figure 19: CDR log example, Contact Closure on page 199

Figure 18: CDR log example, successful ARS calls

```
G250-SLS(super)# show logging cdr file content

02/18/2005,10:46:35:CDR-Informational: 10:46 00:00 A 700 50029555 52001 v301

02/18/2005,10:45:46:CDR-Informational: 10:45 00:00 A 700 50029 52001 v301

02/18/2005,10:45:14:CDR-Informational: 10:45 00:00 A 700 52 52001 v301

02/18/2005,10:44:35:CDR-Informational: 10:44 00:00 A 700 445200 52001 v301

02/10/2005,13:20:23:CDR-Informational: 13:20 00:00 A 700 50029 52001 v301

02/10/2005,13:20:15:CDR-Informational: 13:20 00:00 A 700 50029 52000 v301

02/10/2005,13:20:05:CDR-Informational: 13:20 00:00 A 700 44 52000 v301

02/10/2005,13:19:59:CDR-Informational: 13:19 00:00 A 700 44500 52000 v301
```

An interpretation of the first entry in Figure 18 is:

- Date (**02/18/2005**) of log entry
- Time (**10:46:35**) of log entry
- **CDR-Informational** is the category (to aid sorting).
- **10:46** is the time that the call was placed
- **00:00** is the duration of the call in minutes and seconds or **99:99** if the duration is greater than 99 hours.
- **A** is the condition code.
- **700** is the FAC or TAC number.
- **50029555** is the dialed number.
- **52001** is the extension that originated the call
- **v301** indicates the port through which the call was routed.

Figure 19: CDR log example, Contact Closure

```
G250-SLS(super)# show logging cdr file content

07/27/2005,03:59:24:(0 0 0:15:5)CDR-Informational: July 27 03:59 B 15840 PULSE 003 2
```

An interpretation of the entry in Figure 19 is:

- Date (**07/27/2005**) and time (**03:59:24**) record when the feature was activated.
- **B** is the condition code.
- **15840** is the extension that activated the feature.
- **PULSE** indicates the Contact Closure operation (could also be **OPEN** or **CLOSE**)
- **003** is the media gateway number.
- **2** is the Contact Closure number.

SLS administration procedures

SLS is installed when the media gateway is installed. However, before SLS can actually work, the provisioning data from the PIM tool must have been pushed down to the media gateway or the gateway is manually configured for SLS (see Manually configuring the SLS data on the media gateway on page 208). See these topics for more information about the provisioning data:

- Communication Manager administration on page 200)
- NMC and PIM administration on page 202 or data set from the procedure, Manually configuring the SLS data on the media gateway on page 208.

Communication Manager administration

Two Communication Manager forms must be administered for SLS:

- Station form

```
change station 8003                                      Page   1 of   4
                                    STATION

Extension: 8003                        Lock Messages? n           BCC: 1
     Type: 4620                        Security Code:              TN: 1
     Port: IP                          Coverage Path 1:           COR: 1
     Name:                             Coverage Path 2:           COS: 1
                                       Hunt-to Station:

STATION OPTIONS
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 8003
            Speakerphone: 2-way               Mute button enabled? y
        Display Language? English                Expansion Module? n

  Survivable GK Node Name:                        Media Complex Ext:
          Survivable COR: internal                     IP SoftPhone? N
    Survivable Trunk Dest? y
```

- **Survivable GK Node Name** field supports an H.323 gatekeeper in survivable mode, allowing IP stations to register and subsequently originate/receive calls from other endpoints in this survivable calling zone. This field can contain any node-name administered on the IP Node Names (**`change node-names ip`**) form or be blank (default). When administering the node name, ensure that the IP address associated with the name that you are assigning is that of the G250 Media Gateway.

  Communication Manager adds this IP address to the end of the Alternate Gatekeeper List that is automatically delivered to the IP station and stored in its internal memory during its initial registration with Communication Manager. The IP phone uses this list to find an alternate gatekeeper when registration to the primary server is lost, and it is essential that the IP address on the Node Name form is that of SLS, otherwise the IP phones cannot register when the H.248 link is down.

  If the IP phones are configured to use a local DHCP server for IP address assignments, the server must have its Option 176 programmed with the addresses of the primary Communication Manager gatekeepers, providing a destination for H.323 RAS discovery messages. When an IP phone reboots (for example, a power loss), it relearns and searches the Option 176 list for a gatekeeper. To optimize the SLS recovery strategy place the IP address of the G250 Media Gateway (used by the SLS gatekeeper) at the end of the Option 176 list.

- **Survivable COR** field places a restriction level for stations to limit certain users to certain types of calls:

  - **Emergency** – this station can only be used to place emergency calls that are defined on the Survivable ARS Analysis Table (Figure 20: SLS / ARS page on page 204).

Important:

SLS permits 911 calls, but the specific location information is not transmitted to the Public Service Answering Point (PSAP) but only the general trunk-identifying information. Emergency personnel will have a general location associated with the trunk (for example, a building address), but nothing more specific like the room or office number. Also, If a 911 call disconnects for any reason, emergency personnel cannot reliably call the originator back.

  - **Internal** – this station can only make intra-switch calls (default).
  - **Local** – this station can only make calls that are defined as **locl**, **op**, **svc**, or **hnpa** on the Survivable ARS Analysis Table.
  - **Toll** – this station can place any national toll call which are defined as **fnpa** or **natl** on the Survivable ARS Analysis Table.
  - **Unrestricted** – this station can place a call to any number defined in the Survivable ARS Analysis Table. Those strings administered as **deny** are also denied to these users as well.

  Figure 24: Inherited Class of Restriction (COR) permissions on page 211 shows the hierarchical relationship among these COR permissions.

- **Survivable Trunk Dest?** (y/n, default is y) field allows stations to receive incoming trunk calls or not in the survivable mode. Communication Manager pushes data from these station forms as Dial Route Patterns to the media gateway where they are stored in NVRAM.

- Media Gateway form

```
add media-gateway next                                          Page   1 of 1
                              MEDIA GATEWAY
         Number: 2                              IP Address:
           Type: g250                FW Version/HW Vintage:
           Name:                              MAC Address:
      Serial No:                             Encrypt Link? y
 Network Region:                                 Location: 1
     Registered? n                  Controller IP Address:
  Recovery Rule:                                Site Data:
      Slot   Module Type                Name
       V1:
       V2:
       V3:

 Max Survivable IP Ext:
```

- **Name** field (20 characters maximum) must match the administered name of the G250 (see G250 administration through the command line on page 212, Step 2.

- **Max Survivable IP Ext** field only appears when the **Type** field is **g250**. The limited VOIP resources in the G250 Media Gateway/SLS can only handle so many simultaneous IP endpoint registrations, and this field limits that number (1-60, default is 8).

Important:

Since the VOIP resources on the G250 Media Gateway are limited, the **Max Survivable IP Ext** field should not be greater than 12 for Release 3.1.

NMC and PIM administration

SLS is easily implemented and monitored through Avaya's Integrated Management applications. The Avaya Network Management Console (NMC) is the infrastructure application that "discovers" IP enabled devices and provides fault monitoring. The NMC supports SNMPv1 and SNMPv3 devices and also provides a location from which to launch management applications like the Provisioning and Installation Manager (PIM) application and device managers, as well as other Avaya Integrated Management applications.

One of the uses for the PIM's Device Profile Wizard is administer the frequency and schedule for extracting a subset of the Communication Manager translations (dial plan analysis and destination routing instructions that are necessary for SLS) and delivering the information to a specific SLS-enabled media gateway. If PIM is not available, this translation subset (the SLS data set) can be created manually by using the procedure in Manually configuring the SLS data on the media gateway on page 208 or through SNMP.

To administer Avaya's Integrated Management applications for SLS:

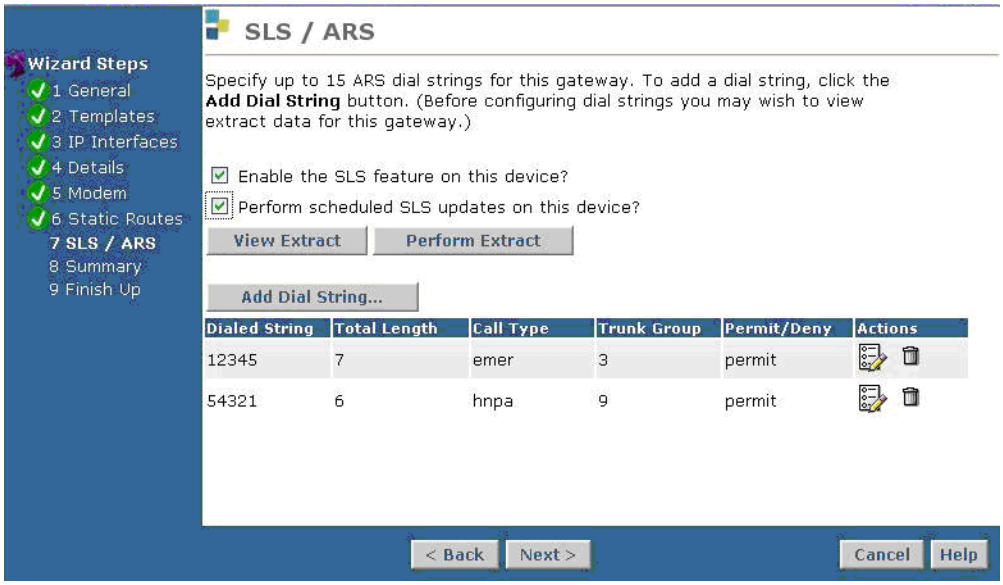
1. Ensure that the Network Management Console (NMC) has discovered the media gateway.
2. Before PIM's automatic scheduled SLS updates will work as expected, set the device parameters for both the server and the gateway in the NMC:
   - Server: Communication Manager login and password

   Note:

   The server must be the first listing in NMC's discovery output. If an ESS node is discovered and listed prior to the main server, the main server's login/password will not permit access to the ESS node.

   - Gateway: SNMPv1/v3 access parameters
   - Gateway: NMC has discovered the gateway's IP address
3. Ensure that the Communication Manager administration on page 200 is complete.
4. Click on the Device Profiles icon/link in the top-level tool bar of the main PIM window. Alternatively, select **PIM Objects > Device Profiles** from the left panel.
5. Click the **New** icon on the Device Profile list page that appears in the right panel of the main PIM window. If this is not a new profile, open the existing profile from the left panel or from the Device Profile list page.
6. Proceed through the Device Profile Wizard to the **SLS / ARS** page (Figure 20: SLS / ARS page on page 204):
   a. Check the **Enable the SLS feature on this device?** box; unchecked means that SLS is disabled.
   b. Check the **Perform scheduled SLS updates on this device?** box which sends the SLS data set to the G250 Media Gateway according to the settings on the SLS Update Schedule form (Figure 22: SLS Update Schedule page on page 206).

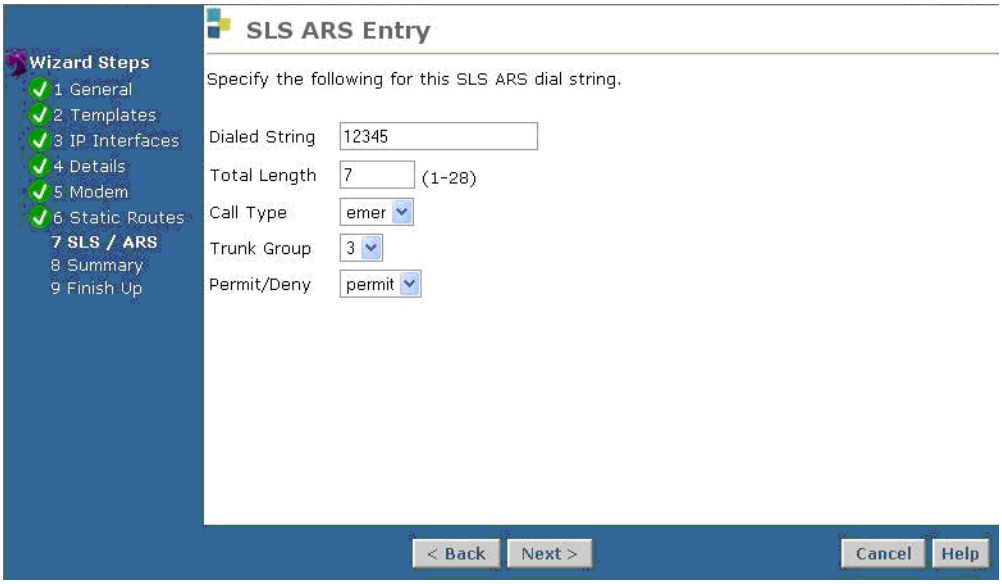
Figure 20: SLS / ARS page



- **View extract** displays the current SLS data set for this G250 Media Gateway.
- **Perform extract** extracts the SLS information from the controlling Communication Manager server for use with this media gateway.
- **Actions** allows you to edit or delete an entry:
  - The paper/pencil icon is the “edit” icon which changes to the ARS Entry page (Figure 21: SLS ARS Entry page on page 205).
  - The trash can icon is the “delete” icon which removes the ARS Entry from the table. In conjunction with the Add ARS Dial String button you can create/edit/delete up to 15 ARS Entries.

7. Click on the **Add Dial String** button to display the SLS ARS Entry page (Figure 21: SLS ARS Entry page on page 205).

Figure 21: SLS ARS Entry page



8. Administer the Automatic Route Selection (ARS) by setting the fields on this page (Table 51).

Table 51: SLS ARS Entry page field options *1 of 2*

Field	Description
Dialed String	Maximum 18 characters: only 0-9, '*' and 'X' or 'x' as a pre-string or mid-string replacement. 'X' cannot be at the end of a dialed string.
Total Length	Length of the dialed string (up to 28 digits). For example, if you entered "123" in the **Dialed String** field, then the **Total Length** field can be any number 3-28. Similarly, if the **Dialed String** field is "123456", then the **Total Length** field can be any number 6-28.
Call Type	**emer** (emergency call)[1] **fnpa** (10-digit NANP call) **hnpa** (7-digit NANP call) **intl** (public-network international number call) **iop** (international operator call) **locl** (public-network local number call) **natl** (non-NANP call) **op** (operator) **svc** (service) See Figure 24: Inherited Class of Restriction (COR) permissions on page 211 for a discussion of the hierarchical relationship among these COR permissions.
	1 of 2

Table 51: SLS ARS Entry page field options *2 of 2*

Field	Description
Trunk Group	Trunk-group number (1-2000), which you can select from the drop-down choices of trunk groups found in the SLS extract from the controlling Communication Manager server.
Permit / Deny	**permit/deny** to indicate whether the call should be permitted or denied
	2 of 2

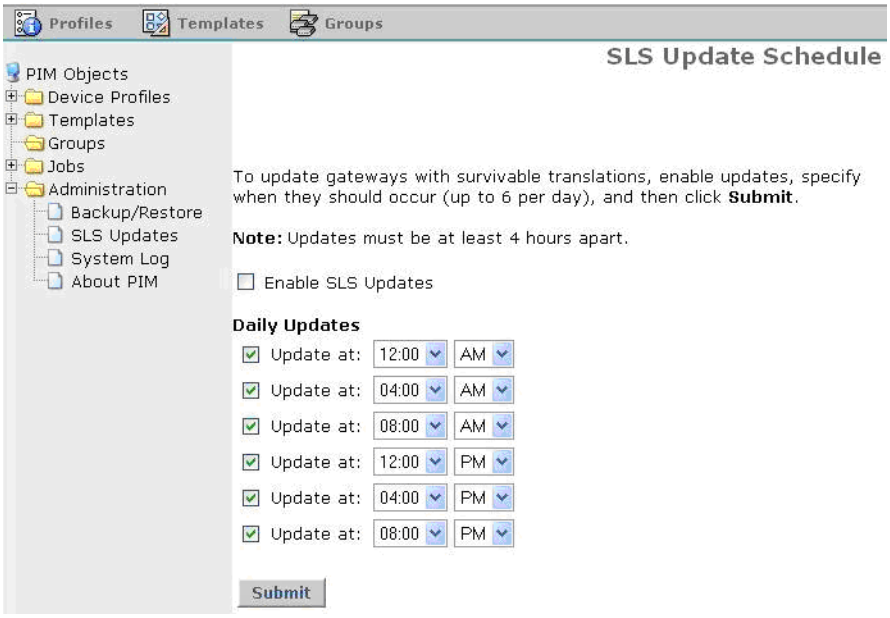
1. Any active, in-service station can dial the emergency access number while in survivable mode. Define the emergency access number on the SLS ARS page (Figure 20: SLS / ARS page on page 204).

Important:

SLS permits 911 calls, but the specific location information is not transmitted to the Public Service Answering Point (PSAP) but only the general trunk-identifying information. Emergency personnel will have a general location associated with the trunk (for example, a building address), but nothing more specific like the room or office number. Also, If a 911 call disconnects for any reason, emergency personnel cannot reliably call the originator back.

9. Use the SLS Update Schedule page (Figure 22) to administer up to six (6) SLS updates per day.

Figure 22: SLS Update Schedule page



a. Check the **Enable SLS Updates** box.

b. Set as many as six (6) Daily Updates.

Note:

The Daily Updates must be at least 4 hours apart.

c. Click on the **Submit** button at the bottom of the page.

10. *Backup the PIM database backup schedule with the **Backup/Restore** page (Figure 23).

Figure 23: Backup/Restore page (PIM)

Note:

Step 10 backs up the PIM database. Avaya encourages users to set a PIM backup schedule/policy independent of the SLS implementation.

Enabling/disabling SLS on the G250 Media Gateway

Prerequisite: The G250 Media Gateway is installed and administered with basic connectivity (for example, name, IP address, etc.)

To enable SLS on the G250 Media Gateway:

1. Log on to the G250 Media Gateway.
2. At the G250 command prompt type **`set survivable-call-engine enable`** to enable SLS on the G250 media gateway.

   The G250 responds with "`Survivable Call Engine is enabled`."

To disable SLS on the G250 Media Gateway:

1. Log on to the G250 Media Gateway.
2. At the G250 command prompt type **`set survivable-call-engine disable`** to enable SLS on the G250 media gateway.

   The G250 responds with "`Survivable Call Engine is disabled`."

Manually configuring the SLS data on the media gateway

This section includes procedures for administering SLS without the help of the Avaya Integrated Management tools:

- Communication Manager administration for manual configuration
- G250 administration through the command line

Communication Manager administration for manual configuration

To administer Communication Manager for SLS and Auto Fallback to Primary:

1. At the Communication Manager SAT type **`change system-parameters mg-recovery-rule 1`** and press **Enter** to display the **System Parameters Media Gateway Automatic Recovery Rule** form.

```
change system-parameters mg-recovery-rule 1                    Page   1 of   1
             SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE
 Recovery Rule Number: 1
 Rule Name: _____________
 Migrate H.248 MG to primary: immediately
 Minimum time of network stability: 3
 WARNING: The MG shall be migrated at the first possible opportunity. The MG may
be migrated with a number of active calls.  These calls shall have their talk
paths preserved, but no additional processing of features shall be honored. The
user must hang up in order to regain access to all features.



 NOTE: set 'Migrate H.248 MG to primary' to Blank to disable rule.
```

2. Type a description of the rule in the **Rule Name** field.
3. Set the **Migrate H.248 MG to primary** field to **immediately**.

   Note:

   This field value (**immediately**) is only one of the four (4) possible choices. See the *Administrator Guide for Avaya Communication Manager* (03-300509) for more information on the values for this field.

4. Submit the form.

5. At the SAT type **`change media-gateway 1`** and press **Enter** to display the **Media Gateway** form.

```
change media-gateway 1                                          Page   1 of   1
                              MEDIA GATEWAY
         Number: 1                              IP Address:
           Type: g250                FW Version/HW Vintage:
           Name:                              MAC Address:
      Serial No:                            Encrypt Link? y
 Network Region:                               Location: 1
     Registered? n                    Controller IP Address:
  Recovery Rule: 1                              Site Data:
      Slot   Module Type                 Name
       V1:
       V2:
       V3:
       V4:




       V8:
       V9:
```

6. Set the **Recovery Rule** field to **1** (example only).
7. Submit the form.
8. At the SAT type **`change node-names ip`** and press **Enter** to display the **IP Node Names** form.

```
change node-names ip                                            Page   1 of   1
                                  IP NODE NAMES
    Name              IP Address           Name              IP Address
_________________    192.168.1  .200                          .   .   .
procr                192.168.1  .201                          .   .   .
(X of X administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

9. In the **Name** field type the G250 name, that is, the name of the survivable gatekeeper node that corresponds to the IP address in Step 10.

   Note:

   Set the name of the media gateway consistent with the **Name** field on the Media Gateway administration form in Communication Manager (**`add media-gateway`**) and with the name used in the **`set system name`** command (G250 CLI).

10. Type the *internal* IP address of the G250 Media Gateway in the **IP Address** field. The internal IP address is that of the survivable gatekeeper, not the gateway's external IP address.
11. Submit the form.

12. At the SAT type **change station *extension*** and press **Enter** to display the **Station** form.

```
change station 8003                                      Page   1 of   4
                                    STATION

Extension: 8003                        Lock Messages? n           BCC: 1
     Type: 4620                        Security Code:              TN: 1
     Port: IP                          Coverage Path 1:           COR: 1
     Name:                             Coverage Path 2:           COS: 1
                                       Hunt-to Station:

STATION OPTIONS
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 8003
            Speakerphone: 2-way               Mute button enabled? y
        Display Language? English                Expansion Module? n

  Survivable GK Node Name:                         Media Complex Ext:
          Survivable COR: internal                      IP SoftPhone? N
    Survivable Trunk Dest? y
```

Survivable GK Node Name - names the gatekeeper to register with when the gateway unregisters (loses call control) with the main server. The media gateway delivers the gatekeeper list to IP endpoints, allowing them to register and subsequently originate/receive calls from other endpoints in this survivable calling zone. This field can contain any node-name administered on the IP Node Names (**change node-names ip**) form or be blank (default).

Survivable COR - places a restriction level for stations to limit certain users to only certain types of calls:

- **Emergency** – this station can only be used to place emergency calls which are defined
- **Internal** – this station can only make intra-switch calls (default)
- **Local** – this station can only make calls that are defined as **locl**, **op**, **svc**, or **hnpa** on the Survivable ARS Analysis Table.
- **Toll** – this station can place any national toll call which are defined as **fnpa** or **natl** on the Survivable ARS Analysis Table.
- **Unrestricted** – this station can place a call to any number defined in the Survivable ARS Analysis Table. Those strings administered as **deny** are also denied to these users as well.

Note:

This field is only for all analog and IP station types.

Figure 24 shows the hierarchical relationship among the calling-restriction categories.

Figure 24: Inherited Class of Restriction (COR) permissions

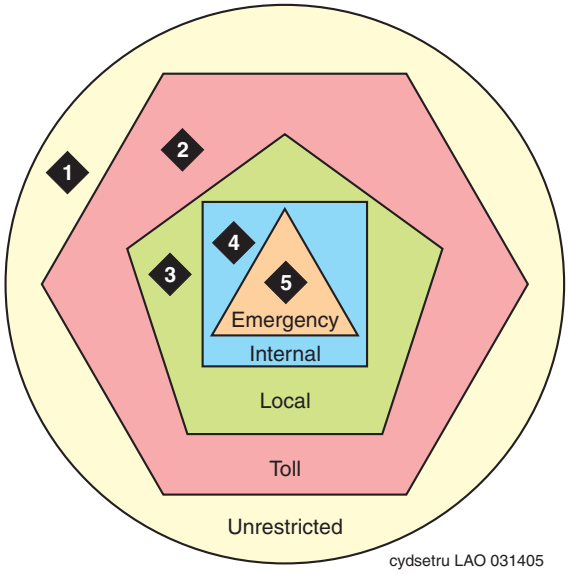


Figure notes:

1. **Unrestricted**: users can dial any valid routable number, except an ARS pattern specifically administered as **deny** (see Figure 20: SLS / ARS page on page 204) ETR functionality and calls through the CO are permitted in this class.
2. **Toll**: users can only dial these call types:
   - **fnpa** (10-digit NANP call)
   - **natl** (non-NANP call)
3. **Local**: users can only dial these call types:
   - **locl** (public-network local number call)
   - **op** (operator)
   - **svc** (service)
   - **hnpa** (7-digit NANP call)
4. **Internal**: users can only dial other stations within the media gateway and the emergency external number (default).
5. **Emergency**: users can only dial the emergency external number.

Survivable Trunk Dest? - (y/n, default is y) allows stations to receive incoming trunk calls or not in the survivable mode. PIM extracts the Communication Manager information, pushes it to the media gateway, and stores it in NVRAM.

13. Submit the form.

    This concludes the Communication Manager administration.

G250 administration through the command line

The command line interface (CLI) has a root-level context of "survivable-call-engine" that provides for administration of only those items pertaining to SLS. After you type **survivable-call-engine** at the CLI prompt and press **Enter**, the prompt changes to indicate that you are in the survivable-call-engine context. Once in this context, two additional sub-contexts provide for station and trunk administration:

- **station** context that is invoked by typing **station *extension class*** and pressing **Enter** to enter a second-level subcontext for administering stations.
- **trunk-group** context that is invoked by typing **trunk-group *tgnum group-type*** and pressing Enter to enter the second-level subcontext for administering trunk groups.

Type **exit** to leave the second-level sub-contexts to return to the "...(**survivable-call-engine)#**" context.

To create the SLS data set on the media gateway through the command line interface:

1. Log on to the G250 Media Gateway.
2. To administer the G250 name type **set system name "*name*"** where ***name*** is typed inside quotes. To remove the administered name type **set system name** and press **Enter**; then rename the G250 with the **set system name** command.

   Note:

   The gateway's administered name must match the name in Communication Manager administration (see Communication Manager administration on page 200)
3. At the G250 command prompt type **survivable-call-engine** and press **Enter** to begin entering SLS data.

   The command line prompt changes to "...(**survivable-call-engine)#**" to indicate that you are in SLS data entry mode. Typing **exit** ends the SLS data entry mode session, and the command line prompt returns to its original state.
4. Administer the station information:

   a. At the G250 command prompt type **station *extension class*** and press **Enter** to enter a second-level subcontext to administer each phone that you want covered by SLS. In this command ***extension*** is a 1-7 digit numeric string (may begin with "0"), and ***class*** is **analog**, **dcp**, or **ip**.

   The command line prompt changes to "...(**survivable-call-engine/station**) to indicate that you are in the station context for SLS administration. Typing **exit** ends the station configuration mode, and the command line prompt returns to its original state. If you want to remove the station from the SLS administration, type **clear extension *extension*** at the command line interface. Type **exit** to leave the second-level "station" context to return to the "...(**survivable-call-engine)#**" context.

   Example

   - **station *1234567 ip*** administers an IP phone with the extension "1234567."

b. Depending on the class (**analog**, **dcp**, or **ip** administration in Step a), type **`set type model`**, where model is a value from Table 52.

Table 52: Class values in SLS station context

analog	dcp	ip
analog2500[1]	dcp2402	ip4601
	dcp2410	ip4602
	dcp2420	ip4602sw
	dcp6402	ip4610sw
	dcp6402D	ip4612
	dcp6408 (default)	ip4620
	dcp6408+	ip4620sw
	dcp6408D	ip4621
	dcp6408D+	ip4622
	dcp6416D+	ip4624
	dcp6424D+	ip4625
	dcp8403B	
	dcp8405B	
	dcp8405B+	
	dcp8405D	
	dcp8405D+	
	dcp8410B	
	dcp8410D	
	dcp8411B	
	dcp8411D	
	dcp8434D	

1. Since there is just one entry, the ***model*** is optional; **analog2500** is the default value.

Examples

- **`set type ip4620`** sets the previously-administered extension "1234567" as an Avaya 4620 IP phone.

c. For **analog** and **dcp** classes only (set in Step a), type **`set port module-port`** for this station, where ***`module-port`*** is a value in Table 53.

Table 53: Module-port values in SLS station configuration mode

G250 model	Analog station ports[1]	DCP station ports
G250-Analog	V305, V306	
G250-BRI	V302, V303	
G250-DCP	V305, V306	V401 through V412
G250-DS1	V302, V303	

1. You cannot select these modules/ports if they are already assigned as DID trunks.

Note:

If the class is **ip** (in Step a), you cannot run this command.

Examples

- **`set port v305`** sets the previously-administered analog station "1234567" to the first physical port on the G250-Analog gateway.
- **`set port v401`** sets the previously-administered dcp station "1234567" to the first physical port on the G-250-DCP gateway.
- **`set port v302`** sets the previously-administered analog station "1234567" to the first physical port on the G250-BRI gateway.

d. Set the class of restriction (COR) for this extension by typing **`set cor cor`**, where ***`cor`*** is any of the following:

- **emergency**
- **internal** (default)
- **local**
- **toll**
- **unrestricted**

See Figure 24 for more information about the hierarchical relationship among the calling-restriction categories. As you move from the most restricted COR (**emergency**) to the least restricted (**unrestricted**), each level increases the range of dialing abilities. For example, **toll** includes the dialing privileges of **local**, **internal**, and **emergency**.

Example

- **set cor *unrestricted*** gives a station unrestricted dialing.

e. If this station is allowed to receive incoming analog loop-start trunk calls, type **set trunk-destination *yes***.

Example

- **set trunk-destination yes** allows a station to receive incoming analog loop-start trunk calls.

f. If this is an IP phone (set in Step a), administer a password by typing **set password *password***, where ***password*** is between 4 and 8 digits in length.

Note:

Passwords are not required for analog or DCP phones, unless an IP Softphone is using the administrative identify of a DCP phone, in which case the password is required.

Example

- **set password *53136*** establishes the password "53136" on a previously-administered IP phone.

g. To allow DCP or IP phones only (set in Step a) to have an expansion module, type **set expansion-module *yes***.

h. For analog phones (set in Step a) that you want SLS to recognize the switchhook flash signal that offers subsequent transfer features, type **set swhook-flash *yes***.

i. Check the extension administration by typing **show**.

The report lists the station parameters:

```
Extension   Type     Port    Cor   Trunk-Des   Exp-Mod     Flash     Password
---------   ----     ----    ----- ---------   -------     -------   --------
49139       ip4620   IPaddr local y           n           -         ********
            ip station registered at address 'aaa.bbb.ccc.ddd'
```

Note:

For currently-registered IP phones or IP Softphones, the IP address is displayed.

j. Type **exit** to leave the extension context in SLS.

5. Administer the trunk groups:

a. At the command line type **trunk-group *tgnum group-type***, where ***tgnum*** is any number 1-2000 and group type is ***loop-start*** (for analog) and ***did*** (for analog).

The command line prompt changes to "...(**sls-trunk-group-<tgnum>**). If you want to remove the trunk group from the SLS administration, type **exit** to leave the second-level "trunk group" context to return to the "...(**survivable-call-engine)#**" context then type **clear trunk-group *tgnum*** at the command line interface.

Note:

You may administer up to 4 analog trunk groups for the G250-Analog and G250-DCP models and only 1 analog trunk group for the G250-BRI and G250-DS1 models. If you exceed these limits, you must delete a trunk group before you can add a new one.

Example

- **`trunk-group 1 loop-start`** establishes an analog loop-start trunk group number 1.

b. At the command line type **`set dial dial-type`**, where ***`dial-type`*** is either **rotary** or **dtmf**.

Example

- **`set dial dtmf`** establishes that the trunk group uses DTMF signalling.

c. At the command line type **`set tac tac`**, where ***`tac`*** is 1-4 digit numeric value (plus initial "#" and "*" on all but rotary dial phones) for this trunk's access code (TAC). The TAC value must be unique among all trunk groups, extension numbers, and ARS Feature Access Code (FAC) strings.

Example

- **`set tac 88`** establishes access to this trunk group by dialing "88."

d. At the command line type **`add port module-port`** to specify the virtual integrated port that is compatible with the G250 model (see Table 54).

Table 54: Module-port values in SLS trunk-group context

G250 model	Analog loop-start trunks	Analog DID trunks
G250-Analog	V301, V302, V303, V304	V305, V306
G250-BRI	V301	V302, V303
G250-DCP	V301, V302, V303, V304	V305, V306
G250-DS1	V301	V302, V303

Example

- **`add port V304`** administers an analog loop-start trunk through port V304 on either the G250-Analog or the G250 DCP.

e. For analog DID trunk groups only, at the command line type **`set supervision sup-type`**, where ***`sup-type`*** is either **immediate** or **wink**.

Example

- **`set supervision wink`** assigns wink-start incoming signaling supervision to a DID trunk group.

f. *For analog DID trunk groups only, at the command line type **set digit-treatment *digit-treat***, where ***digit-treat*** is any of the following values:

- blank (use this value to remove any absorb or insert digit treatment)
- absorb1
- absorb2
- absorb3
- absorb4
- absorb5
- insert1
- insert2
- insert3
- insert4

Example

- **set digit-treatment *absorb1*** removes the first digit from the incoming DID trunk.
- **set digit-treatment *blank*** removes any digit treatment from the trunk group.

g. For analog DID trunk groups only, at the command line type **set digits *digits***, where ***digits*** is the number of digits, to define the inserted digit string.

Note:

The number of digits must agree with the ***digit-treat*** parameter in the **set digit-treatment** command. If the digit-treat parameter is ***insert3*** then the digits parameter for this command be three digits in length.

h. Check the trunk-group administration by typing ***show***.

The report lists the trunk-group parameters:

```
Trunk-Grp   Type       Dial   TAC   Port   Supervision    Dig-Treat    Digits
---------   ----       ----   ---   ----   -----------    ---------    ------
1           loop-start dtmf   99    v301   -              -            -
```

i. Type **exit** to leave the trunk-group context in SLS.

6. At the G250 command prompt type **set dial-pattern *dialed-string length type deny tgnum*** for each SLS dial pattern.

Important:

The trunk group must already exist (see Step 5 above) before you can issue this command.

Examples

- **set dial-pattern *100 4 fnpa false 30***
- **set dial-pattern *200 4 fnpa false 30***

7. Administer the Feature Access Codes (FACs):
   a. At the G250 command prompt type **set fac *feature fac***, where ***feature*** is any of the following:
      - **ars1**
      - **ars2**
      - **hold**
      - **contact-open**
      - **contact-close**
      - **contact-pulse**

      and ***fac*** is a 1-4 digit string that includes the digits "0" through "9," excluding "*" and "#" for analog rotary phones. The ***fac*** string must be unique and must not conflict with station extension numbers and Trunk Access Codes (TACs).

   Examples

   - **set fac *ars2 *9***
   - **set fac *contact-close 8***

   Note:

   The "*" and "#" characters are not available on rotary-dial, analog phones.

8. Use the **set-ip-codec-set** command to select the country-specific G.711 codec (G.711mu or G.711a).
9. If you want to change the maximum allowable IP registrations from the default, use the **set max-ip-registrations *n*** command, where ***n*** is between 1-12.

   Important:

   Since the VOIP resources on the G250 Media Gateway are limited, adjusting the maximum IP registrations above the default value can result in system performance problems.

10. At the G250 command prompt type **exit** to leave the survivable-call-engine context.

    The G250 command prompt reverts to that of the original login.

11. At the G250 command prompt type **set survivable-call-engine *enable*** to enable SLS on the G250 media gateway.
12. At the G250 command prompt type **copy running-config startup-config** to save the changes.

System resets

The following tables describe the duration, causes, and effects of the Media Servers' reset levels:

- Reset Level 1 (Warm Restart) on page 219
- Reset Level 2 (Cold-2 Restart) on page 220
- Reset Level 4 on page 222
- Reset Level 5 (Extended Communication Manager reboot) on page 223

Reset Level 1 (Warm Restart)

Duration	Up to 10 seconds, typically 4 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).

1 of 2

	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 translation** operation is in progress, an SAT-requested warm restart would be aborted. A software-requested warm restart would result in an unsuccessful **save translation** operation and possibly corrupt translations.

2 of 2

Reset Level 2 (Cold-2 Restart)

Duration	Up to 3.75 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.
	Gateways are *not* reset.
	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 translation** 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 translation** operation and possibly corrupt translations.
	Every login, including remote access and system port logins, is dropped.
	Initialization firmware runs diagnostics and displays results on the screen.

1 of 2

	Server memory shadowing is turned off, leaving the standby **server** unavailable for service for up to several minutes.
	Every hardware component is reset *except* • Active TN2312 IPSI in any PN. • Active EI in a non-IPSI connected PN. • SNIs. • SNCs. • 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.
	2 of 2

Reset Level 3 (Communication Manager reboot)

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

Reset Level 4

Communication Manager reload

CAUTION:

Reset Level 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	System software (boot image) is reloaded and every process is re-initialized.
	Communication Manager administration (translations) are reloaded from the hard disk.
	Before reboot, the system attempts to save the alarm and error logs.
	After reboot, error and alarm logs are restored. 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 Avaya products.

S8300/G700 system reset

System resets in the S8300 Media Server in a G700 Media Gateway are no different from other Avaya Media Servers. Although translations might 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.

After Media Server 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 begins.

Audits

Six (6) minutes after an S8300 reset Communication Manager conducts an in-line Media Module audit (Test #1583) that compares the Media Modules present with those that were present before the system reset.

Chapter 5: General troubleshooting

- Introduction
- Knowing when there is a problem
- Viewing the alarm and event logs
- Interpreting the Communication Manager report
  - Viewing the SAT log
  - Viewing the Web interface logs
- Diagnosing the problem
- Repairing or escalating the problem

Introduction

This chapter contains information about how to better understand system problems that are reported through Avaya Communication Manager's maintenance subsystem. While pro-actively testing in the background and gathering and reporting vital information from several concurrent processes, Communication Manager maintenance can often notify you of problems before failures occur: variations in environments (temperature, voltages, fan speeds), and of irregularities in connections or services.

In general, two steps are needed to resolve a problem:

- Identify the location of the problem (IP telephone, network, PBX, and so on), by using alarms and the state information of devices along with any administration information that you gather.
- Repair the problem: correct parameter provisioning, upgrade software or firmware, or replace hardware.

Alarm and event log

Figure 25 shows several processes that report to the system logs.

Figure 25: Maintenance subsystem

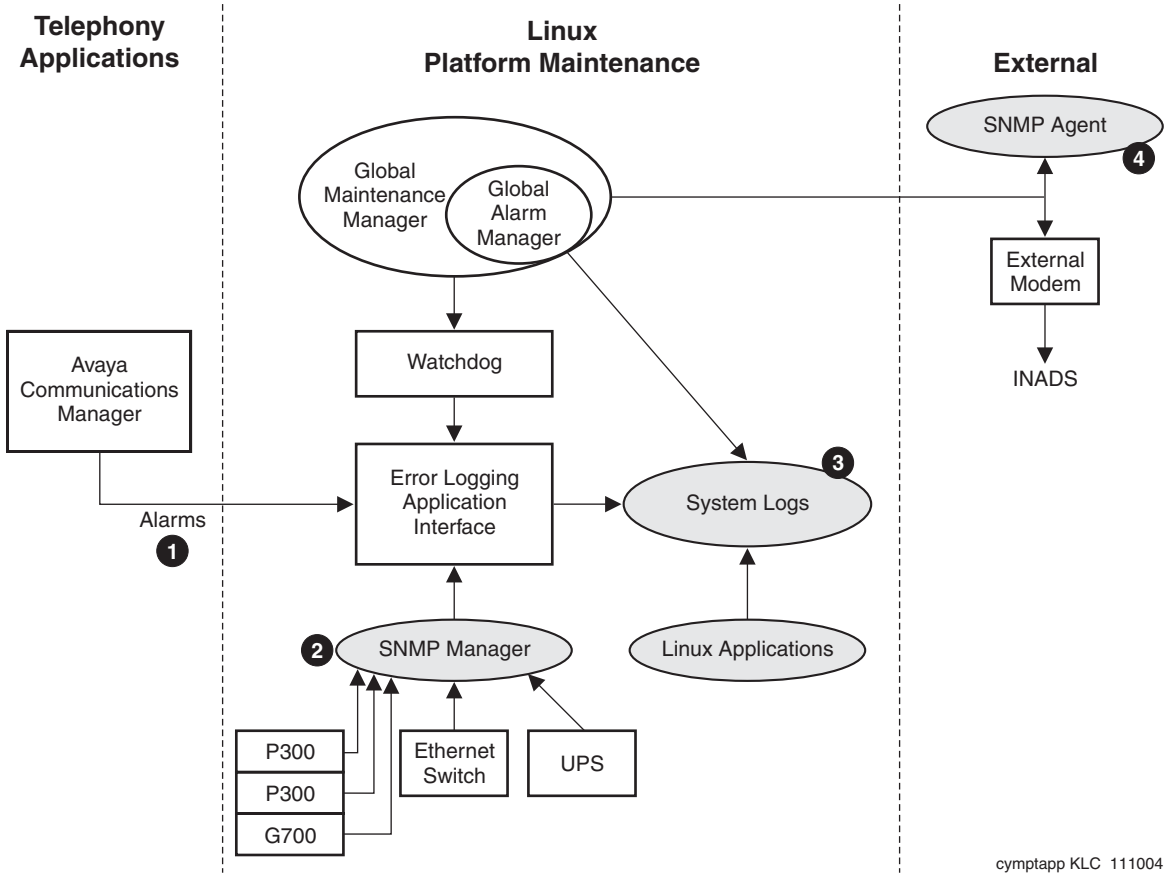


Figure notes:

1. Communication Manager alarms can be viewed from the:
   - SAT by using the **`display alarms`** command.
   - Web interface by selecting **Alarms > Current Alarms**.
2. SNMP Manager sends traps to SNMP Agent application
3. System logs can be viewed through the Web interface by selecting **Diagnostics > System Logs**.
4. SNMP Agent application

The maintenance subsystem gathers detailed alarm/error information from three major processes:

- Avaya Communication Manager—the telephony application
- Server-based maintenance subsystem applications
- Linux server

Figure 25 shows that the system log is the main repository for reporting alarms. You can view the Alarm Log through any of the three different interfaces listed in Table 55.

Table 55: Maintenance interfaces

Interface	Connection	Description
Maintenance Web pages	Network through server's IP address	Recommended for most maintenance-related functions and information. The report is divided into two main sections: • Communication Manager alarms • Server alarms See Viewing the Web interface logs for more information about how to access and interpret the various logs.
System Access Terminal (SAT)	Avaya Site Administration through the network or dedicated port on server	Main Communication Manager interface from which you can launch an: • Event report: logs and explains specific events that occur during call processing. Often, these are not problems that require immediate action, but are informational. • Alarm report: the main source for Communication Manager alarms, which include out-of-range temperature or voltage values, broken or fluctuating connections, defective hardware, etc.
Command Line Interface (CLI)	Telnet session through the network or dedicated port on server	Recommended only when the Maintenance Web pages or the SAT are not accessible. See Commonly-accessed directories and files on Linux servers on page 228 for information about the types of files and logs and their locations.

Commonly-accessed directories and files on Linux servers

Table 56 describes the directories and some useful log files in each that can be quick indicators of problems. These files are not useful to the general user, as much of the information is contained in SAT reports or Web interface logs and reports. However, the information is presented here for situations in which the SAT and Web interface might not be available.

CAUTION:
Do not directly manipulate (change) the files in Table 56.

Table 56: Directories and files for troubleshooting *1 of 3*

Directory	File	Description
/etc/opt/ecs	ecs.conf	This file is the configuration file for the switch and is essential for Communication Manager Applications to run correctly. The file is populated when you configure the server through the Maintenance Web interface. Flags that are set incorrectly in this file can cause numerous problems in the switch.
	servers.conf	This file contains information on the IP addresses of the servers and the control networks. This information is useful for troubleshooting possible network problems. This file is populated by using the **Server Configuration > Configure Server** option on the Maintenance Web interface.
/etc/hosts		This file contains the IP addresses of all IPSIs, Cajun-family devices, and servers in the system. This information is useful for troubleshooting possible network problems. This file is populated by using the **Server Configuration > Configure Server** option on the Maintenance Web interface.
	lspList	This file is usually 0 bytes long, unless one or more Local Survivable Processors (LSPs) are registered to this server. If LSPs are registered, this file contains the IP addresses of the LSPs to which Communication Manager has tried to send the translation files. This file is populated by registering LSPs.

1 of 3

Table 56: Directories and files for troubleshooting *2 of 3*

Directory	File	Description
/var/log/ecs		This directory contains three very useful types of files: • ecs log files • Commandhistory • wdlog
	ecs log files	These log files are marked by the date on which the log files occur and provide information about Communication Manager and various Linux processes. However, this information might not be directly useful.
	Commandhistory	This file contains the history of commands that are issued on the server. This file shows such things as when server interchanges were done, when patches were applied, and when servers were started and stopped. Note that this file does not record every command that is run at the Linux CLI but is populated by the various command interfaces.
	wdlog	This file is the watchdog log, the process in Communication Manager that watches over all other processes to ensure proper behavior. This log outputs occupancy profiles on a per-process basis if the system is running at high occupancy. This file is populated by the Watchdog process.
/var/log/ messages		This file contains more information about system behavior, including information on modems, security, and traps.
/var/crash		If the core-vector is set on a server that is running Communication Manager, a core dump is generated on system restarts for Linux-based servers. See Core dumps and mini-core dumps for some basic information about core dumps. This file is populated by various Linux processes.
		2 of 3

Table 56: Directories and files for troubleshooting *3 of 3*

Directory	File	Description
/var/log/defty/dumps		If the core vector is not set on a server that is running Communication Manager, a mini core dump (smaller version of the core dump) might be generated on restarts. This directory contains core dumps on Linux-based servers. See Core dumps and mini-core dumps for some basic information about mini core dumps. This file is populated by various Linux processes.
	Core dumps and mini-core dumps	A core dump is a file that contains a snapshot of the memory image of the server at the time that the core dump is generated. A core dump is required to debug system failures in depth. System failures can vary from a single process restart to a reload of the server. To generate a core dump, you set a flag in the low-level maintenance monitor (LMM) on legacy system (G3r, si, and csi). This flag can be enabled or disabled. When enabled, this flag can generate core dumps under various conditions. On Linux-based servers, the /var/crash directory contains core dumps. A mini core dump is usually generated without setting any flags. However, a mini core dump generates less useful information than a core dump. On Linux-based servers the /var/log/defty/dump contains mini core dumps.
		3 of 3

Knowing when there is a problem

Having the answer to the following question determines whether or not you can benefit from the information that follows in this chapter:

Did the system operate correctly before the problem arose?

- If the answer is no, then review end-to-end administration (for example, connection negotiation, synchronization reference), consult with Avaya Network Optimization to adjust traffic and configuration as necessary, and answer these follow-up questions:
  - *Has the network had a voice readiness assessment?* If not, the network might not be compatible with the voice network readiness guidelines for Avaya products.
  - *Has the network changed since the network assessment?* Any network modifications should follow the network readiness guidelines.
- If the answer is yes, then the information that follows can help you diagnose and possibly repair your system.

Depending upon how you have administered your system, you can become aware of a problem through:

- Equipment indicators
- User-reported problems
- Status reports and activity tracing

Equipment indicators

You can see or discover that you have an alarm or error by looking at or trying to use the physical equipment:

- Avaya media servers, media modules, and circuit packs have color-coded LEDs to indicate the presence of alarms and the level. See LEDs in *Maintenance Alarms Reference (03-300430)*.
- Avaya phones can have administered buttons to indicate certain types of alarms (see *Administrator Guide for Avaya Communication Manager, 03-300509*).

User-reported problems

Phone users report a wide variety of problems that they experience, but nearly all of them fall into one of these categories:

- Performance issues: no lights/dial tone, unable to make calls, poor voice quality, dropped calls/conferences
- Equipment issues: no lights/dial tone, unable to make calls, unable to access or ping equipment
- Connection/services issues: no lights/dial tone (IP endpoints); unable to make calls (all or part) (T1/E1, tie trunks, data w/ QoS/SLAs, etc.)

Pinpointing the location of the problem as precisely as possible so that any repair actions require minimal effort reduces the repair costs and minimizes the impact on noncorrupted service. Therefore, gathering the pertinent information is essential to the troubleshooting process.

If you receive notification of a problem from a user within the system:

1. Collect all pertinent information:
   - Where is the user (building, floor, country, etc.)? What is the extension?
   - Is anyone else experiencing this problem (same floor, building, country, etc.)?
   - Exactly what happened? What kind of call? When? To whom (internal or external call)? What keystrokes, details, etc.
   - Is the problem reproducible? For instance, if a user is trying to call an external public telephone number and getting block, do they get blocked every time they try? If the problem is reproducible, it is much easier to diagnose and repair.
2. Look up connection/configuration information (**`status station`**) as shown in Figure 26: Status station form, page 1 on page 232 through Figure 28: Status station form, page 3 on page 234.

   Note:

   Different fields might appear on this screen, and some fields might appear on different pages depending on your system configuration. Figure 26 is appears as an example only.

Figure 26: Status station form, page 1

```
status station 32014                                        Page   x of   x
                              GENERAL STATUS
     Administered Type: 4620                Service State: in-service/on-hook
        Connected Type: 4620           Parameter Download: complete
             Extension: 32014                SAC Activated? no
                  Port: S00030            User Cntrl Restr: none
           Call Parked? no                Group Cntrl Restr: none
      Ring Cut Off Act? no               CF Destination Ext:
Active Coverage Option: 1

          EC500 Status: N/A         Off-PBX Service State: N/A
       Message Waiting:
       Connected Ports:




                                            HOSPITALITY STATUS
                                         Awaken at:
                                          User DND: not activated
                                         Group DND: not activated
                                       Room Status: non-guest room
```

   a. Does the **Service State** field read **in-service**? If yes, proceed; if no, determine why not)
   b. Is the **Extension** field correct? That is, are you looking up the information for the correct phone?

c. Write down the **Port** assignment.

d. If the user-report is that the station cannot be called or does not ring, check to ensure that the station:

- Is not call-forwarded (**CF Destination Ext** field is blank).
- Does not have Send all Calls activated (**SAC Activated?** field is **no**).
- Does not have Ring Cut Off activated (**Ring Cut Off Act** is **no**).
- Does not have a user on Group Controlled Restriction (**User Cntrl Restr** and **Group Cntrl Restr** fields are **none**). This controlled station restriction can render the station outgoing- or incoming-restricted, or completely disabled (both outgoing- and incoming-restricted).
- HOSPITALITY STATUS: the user or group Do Not Disturb are not active (the **User DND** and **Group DND** are **not activated**.

e. Scroll to the CONNECTED STATION INFORMATION section.

Figure 27: Status station form, page 2

```
status station 32014                                          Page   x of   x
                                GENERAL STATUS

CONNECTED STATION INFORMATION
                Part ID Number: unavailable
                 Serial Number: unavailable

          Station Lock Active? no

UNICODE DISPLAY INFORMATION
          Native Name Scripts: N/A
      Display Message Scripts: 0x00000001:Latn
    Station Supported Scripts: 0x00000007:Latn;Lat1;LatA
```

f. Is the **Station Lock Active** field **no**? If yes, proceed; if no, unlock the extension (change the field to **no**) and try a call from it.

g. Scroll to CALL CONTROL SIGNALING section of the form (Figure 28).

Figure 28: Status station form, page 3

```
status station 32014                                        Page   x of   x

                                CALL CONTROL SIGNALING
                  Switch                        IP                        IP
                  Port      Switch-end IP Addr:Port     Set-end IP Addr:Port
     IP Signaling: 02A1717  135.122. 47.152   :1720     135.122. 47.102:3863
            H.245:
        Node Name:           mc_clan2
   Network Region:           1                          1
                                AUDIO CHANNEL
                  Switch                        IP                        IP
                  Port      Other-end IP Addr :Port     Set-end IP Addr:Port
            Audio:
        Node Name:
   Network Region:
    Audio Connection Type: ip-tdm
   Product ID and Release: IP_Phone   2.100
  H.245 Tunneled in Q.931? does not apply
      Registration Status: registered-authenticated
              MAC Address: 00:04:0d:27:67:fa
       Native NAT Address: not applicable
 ALG - NAT WAN IP address: not applicable
      Authentication type: DES-56-plus
```

h. If this is an IP endpoint, write down all of the following **IP Signaling** information:
   - **Switch Port** (02A1717 in this example)
   - **Switch-end IP Addr:Port** (135.122.47.152:1720 in this example)
   - **Set-end IP Addr:Port** (135.122.47.102:3863 in this example)

i. Check the **Audio Connection Type** field (ip-tdm)

j. Check the **Registration Status** field (registered-authenticated)

3. Through your understanding of your system's configuration, try to determine what part(s) of the system might be affected.

Status reports and activity tracing

You will often need additional information about the state of the network, such as router and switch port statistics or router access control lists. You can get this information by directly logging into the IP network or by using a protocol analyzer to monitor traffic.

Several commands that are helpful in troubleshooting IP Telephony problems are listed in Table 57 along with their usage.

Table 57: Troubleshooting commands and their usage

Command	Use
list trace station	This command traces the behavior of a particular station. It shows off-hook status, call setup and teardown messages, call routing, and call performance (for IP sets only). Every 10 seconds it displays packet loss and jitter statistics for the previous 10 seconds to assist in voice-quality troubleshooting or calls that fail to set up properly.
list trace tac	This command operates similar to **`list trace station`**, but it operates on trunks. In addition to call setup, teardown, and routing, it also lists voice-quality statistics in 10-second increments. This is useful for troubleshooting call routing problems or voice-quality problems across IP trunks.
list trace ras	This command allows an administrator to watch the state of the RAS messages that Communication Manager is processing. This can either be limited to a single station or expanded to the whole system. It shows registration, keepalive, and unregistration requests. This is useful when IP Telephones are rebooting spontaneously or fail to register.
status station	This command shows a snapshot of the state of an individual station. It lists registration status, the CLAN and media processor or IP endpoint that is connected to an IP station, and lists 10 seconds of voice-quality (packet loss and jitter) information. It also shows whether the call is shuffled, hairpinned, or connected to the TDM bus.
status trunk	This command shows a snapshot of the state of an individual trunk. It lists the far-end CLAN and media processor or IP endpoint that is connected to an IP trunk, and lists 10 seconds of voice-quality (packet loss and jitter) information. It also shows whether the call is shuffled, hairpinned, or connected to the TDM bus.

Viewing the alarm and event logs

Using the alarm and event logs helps you isolate the source of the problem, usually through the “divide and conquer” approach which involves:

- Segmenting the configuration
- Testing equipment/connections
- Interpreting the results
- Confirming/denying the relevance of the results
- Repeating until isolation successfully points to the problem source

Tip:
It is essential that you have a thorough knowledge of the equipment and configuration and have pertinent information at hand to quickly and effectively diagnose and fix problems.

Although careful examination of the alarm/event logs is the key to understanding what the problem is, you probably do not want to look at the entire log for these reasons:

- Too much data -- the cause of the problem is likely contained in a few lines of the log.
- Not all relevant -- not within the time frame, not in a particular port network, or assigned to a particular CLAN.

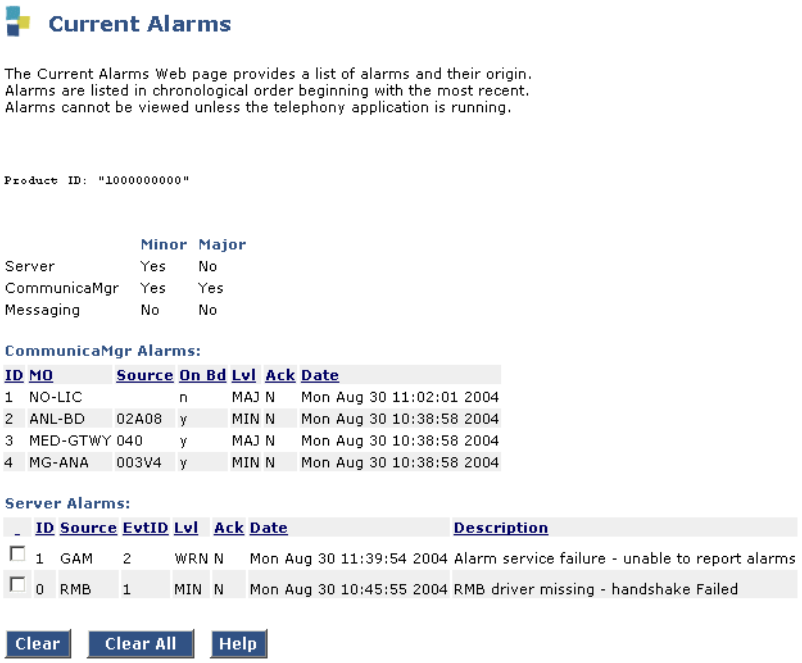
Depending on the type of interface you are using, go to:

- Viewing the Maintenance Web page log
- Viewing the SAT log

Viewing the Maintenance Web page log

Figure 29 shows an example of an alarm log as seen from the Maintenance Web interface.

Figure 29: Current Alarms page



The top part of the report shows the current Communication Manager alarms, and the bottom part shows the current Linux Server Alarms.

Note:

Clearing alarms on this page does not actually resolve them, it only clears the alarm history.

Viewing the SAT log

The SAT interface allows you to use sorting and filtering capabilities to narrow your search of the logs:

- Alarm report
- Event report

Alarm report

Use the Alarm Report form to filter or sort the Alarm Log.

1. At the SAT type **`display alarms`** and press **Enter**.

   The **Alarm Report** form displays (Figure 30).

Figure 30: Alarm report form

```
                                ALARM REPORT

    The following options control which alarms will be displayed.
      ALARM TYPES

                 Active? y    Resolved? n
                  Major? y       Minor? y      Warning? y

      REPORT PERIOD

                Interval: a      From:   /  /  :      To:   /  /  :

      EQUIPMENT TYPE ( Choose only one, if any, of the following )
                     Media Gateway:
                           Cabinet:
                      Port Network:
                      Board Number:
                              Port:
                          Category:
                         Extension:
            Trunk ( group/member ):     /
```

2. Put values in the various fields to display only the alarms that you want:

Field	Values and description
Active	**y** displays active (unresolved) alarms **n** omits (unresolved) alarms
Resolved	**y** displays previously resolved alarms **n** omits previously resolved alarms
Major	**y** displays major alarms **n** omits major alarms
Minor	**y** displays minor alarms **n** omits minor alarms

1 of 2

Field	Values and description
Warning	**y** Displays warning alarms **n** Omits warning alarms
Interval	**h**(our) **d**(ay) **w**(eek) **m**(onth) **a**(ll)
From To	Use Month/Day/Hour/Minute format in both the **From** and **To** fields to define a time range. If no **To** date is entered, all active alarms after the **From** date display.
Media Gateway	Media gateway number (1-250)
Cabinet	Cabinet number (1-64)
Port Network	Port network number (1-64)
Board Number	Cabinet/carrier/slot/ address. Examples: • **01A08** means cabinet 1, carrier A, slot 8. • **001V4** means media gateway 1, slot 4.
Port	Cabinet/carrier/slot/port address. Examples: • **01A0801** means cabinet 1, carrier A, slot 8, port 1. • **001V404** means media gateway 1, slot 4, port 4.
Category	See Alarm and Error Categories in *Maintenance Commands Reference (03-300431)* for a list of the categories and the maintenance objects included in each.
Extension	Enter the assigned extension number.
Trunk (group/member)	Enter the trunk group number in the field to the left of the slash (“/”) and the trunk member number in the field to the right of the slash.

2 of 2

3. Press **Enter** to submit the form.

   The **Alarm Report** displays. See Interpreting the Communication Manager report on page 243 to continue diagnosis of the problem.

Event report

Use the Event Report form to filter or sort the Event Log.

1. At the SAT type display events and press **Enter**.

   The Event Report form (Figure 31) displays.

Figure 31: Event report form

```
                                EVENT REPORT

     The following options control which events will be displayed.

        EVENT CATEGORY

           Category:

        REPORT PERIOD

           Interval: a      From:    /  /   :   To:    /  /   :

        SEARCH OPTIONS

                          Vector Number:
                             Event Type:
                              Extension:
```

2. Put values in the various fields to display only the alarms that you want:

Field	Values and description
Category	**all** - displays events in all categories **contact-cl** - displays contact closure events (relay open, closed, or pulsing) **data-error** - displays internal software events (for example, companding mismatch, read/write **denial** - displays denied call processing events **meet-me** - displays errors generated while using Meet-Me conferencing **vector** - displays errors generated during call vector processing
Interval	**h**(our) **d**(ay) **w**(eek) **m**(onth) **a**(ll)
From To	Use Month/Day/Hour/Minute format in both the **From** and **To** fields to define a time range. If no **To** date is entered, all active alarms after the **From** date display.
Vector Number	Vector number (1-999)
Event Type	Event number (0-9999)
Extension	Enter the assigned extension number.

3. Press **Enter** to submit the form.

   The **Event Report** displays. See Interpreting the Communication Manager report to continue diagnosis of the problem.

Viewing the Web interface logs

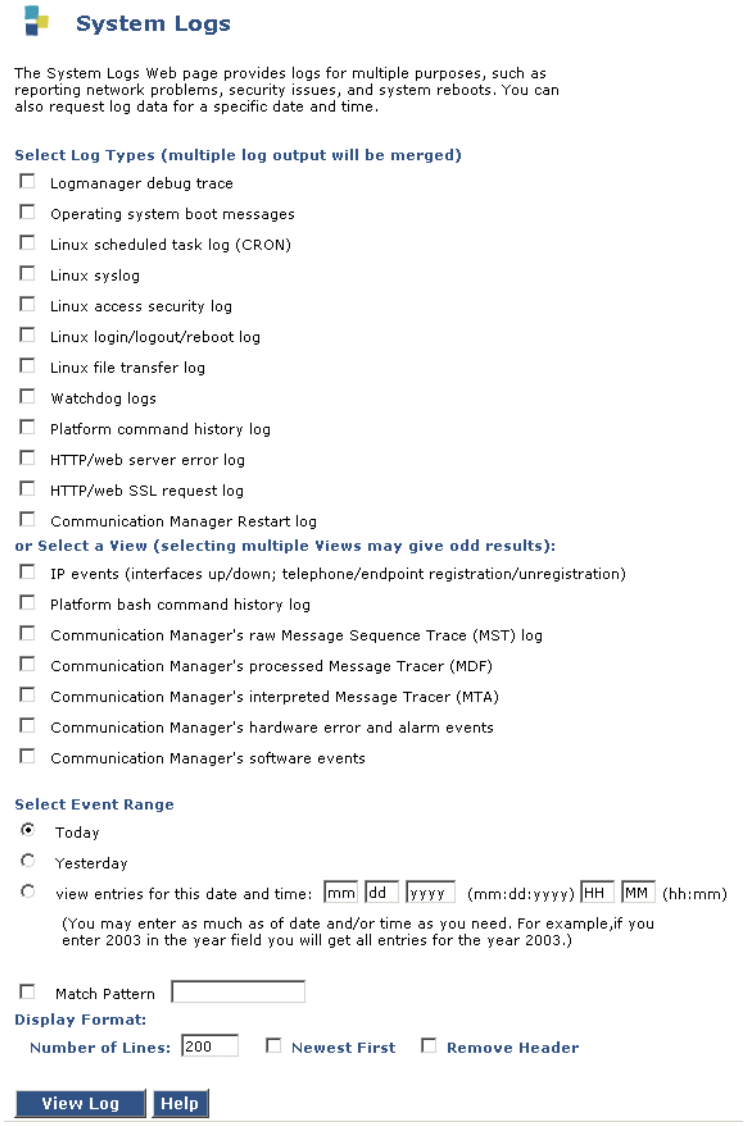
4. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

5. From the left side select **Diagnostics > System Logs**.

   The **System Logs** page (Figure 32: System Logs page on page 242) displays.

Figure 32: System Logs page



6. In the **Select Log Types** section select **Communication Manager hardware error and alarm events**.
7. Click on the **View Log** button at the bottom of the page.

   The View Log page displays 200 lines of the most recent log entries.
8. The Interpreting the Web interface log entries section describes the various log entry types.

Interpreting the Web interface log entries

Each line of the log consists of common information available on any line of the tracelog followed by event-specific information. The beginning of each line of the IP events log is exactly the same as those of any line on the tracelog. The generic information is distinct from the failure-specific information in that it is separated by colons(:) as in the following example:

```
20030227:000411863:46766:MAP(11111):MED:
```

Interpret the information as follows:

- **20030227** is the date (February 27, 2003)
- **000411863** is the time (00 hours, 04 minutes, 11 seconds, 863 milliseconds (ms) or 00:04:11 AM).
- **46766** is the sequence number of this entry.
- **MAP(11111)** is the name and number of the process generating the event.
- **MED** is the priority level (medium).

Following the generic information the alarm information appears in brackets []. See Interpreting the Communication Manager report to continue diagnosing the problem.

Interpreting the Communication Manager report

Both the SAT report and the Web interface Server Alarms page contain similar information about Communication Manager's hardware errors and alarms. Along with the information that you have gathered in the section titled Knowing when there is a problem on page 230 and the information contained in the logs, you need to

- Find the "first cause" (initial failure) versus any consequences that occurred as a result of the initial failure.
- Use timestamps to help reconstruct the incident, looking carefully for the "first cause" and the consequential alarms within seconds of each other.

Figure 33 shows an example of a SAT alarm log that illustrates the cause-and-effect relationship between the “first cause” and its consequences.

Figure 33: Alarm report (log) from SAT

```
                                ALARM REPORT

Port        Maintenance  On   Alt      Alarm    Svc    Ack?  Date         Date
            Name         Brd? Name     Type     State  1 2   Alarmed      Resolved

SERVER      PLAT-ALM     n             MAJOR           y     08/30/15:52  00/00/00:00
003         MED-GTWY     y             MAJOR           y     08/30/16:00  00/00/00:00
01          POWER        y             MINOR           y     08/30/15:53  00/00/00:00
01A19       UDS1-BD      n             WARNING               08/30/15:53  00/00/00:00
01A19       UDS1-BD      n             WARNING               08/30/15:53  00/00/00:00
```

Figure 33 shows that the Major alarms appear first in the log, followed the Minor and Warning alarms.

Using the timestamp to “divide and conquer,” note the following:

- 1st event (1st entry): `SERVER PLAT-ALM n MAJOR y  08/30/15:52 00/00/00:00`
- 2nd event (3rd entry): `01  POWER  y MINOR y  08/30/15:53 00/00/00:00`

  This indicates that the media gateway encountered a power outage at 3:53PM, however the log shows a major gateway alarm as the second entry because of the Major alarm level.
- 3rd event (2nd entry): `003  MED-GTWY  y MAJOR y  08/30/16:00 00/00/00:00`
- The subsequent warning alarms that occurred within the next two minutes are most likely consequences of the power outage.

Diagnosing the problem

Many strategies can identify the location of a IP Telephony problem. For example, one could pinpoint the location of a problem in the following ways:

- Analyze protocol layers from the bottom up, protocol layer after protocol layer, starting at the physical layer.
- First analyze the perceived voice impairments (echo, delay, and voice clipping) if any, and then analyze signaling and network impairment problems.
- Start with a solution that is most likely to resolve the problem, followed by less likely solutions if necessary.

- Look at large behavioral patterns:
  - *Do other IP Telephones on the same subnetwork/VLAN, floor, switch port, router MedPro, CLAN, network region, campus, software or firmware version, or Communication Manager version have the same problem?* Similar problems with multiple IP Telephones might indicate shared resource problems such as power problems, Ethernet switch or IP router problems, or remote connectivity WAN problems. It may also indicate software or firmware version problems.
  - *Does the problem repeat at a specific time of day?* At specific times, the network load may be higher, which might cause your system to run out of IP Telephony resources.
- Look for simple solutions, for example, if only one IP telephone has a problem:
  - If exchanging the IP telephone solves the problem, then the IP telephone is likely the source of the problem, unless the problem is intermittent.
  - If the problem is solved when the IP telephone is connected to a different Ethernet switch port or IP router port, then the IP telephone is not the problem.
- *Are compatible codecs used?* Review the network region administration for end-to-end compatibility.

Repairing or escalating the problem

If you do not understand the problem, you can:

- Investigate more; check services status for potential service-provider outage, etc.
- Status check other telephony and data equipment on same network
- Escalate the problem to your technical support representative.

If your study of the logs and other status information has clarified the problem and you want to begin repairing the system, use the information in this section and in *Maintenance Alarms Reference (03-300430)* and *Maintenance Commands Reference (03-300431)*.

To illustrate a repair procedure using the information in the Maintenance books, we'll use an example that guides you through entire process.

1. At the SAT type **`display alarms`** and press **Enter**.

   The **Alarm Report** form displays. Input whatever sort parameters help you view the log (see Alarm report on page 238).

```
                                ALARM REPORT

Port       Maintenance  On   Alt      Alarm    Svc    Ack?  Date         Date
           Name         Brd? Name     Type     State  1 2   Alarmed      Resolved

S00000     DIG-IP-S     n    40000    WARNING  IN           09/24/16:59  00/00/00:00
S00004     DIG-IP-S     n    40002    WARNING  IN           09/24/16:59  00/00/00:00
S00009     DIG-IP-S     n    2553203  WARNING  IN           09/24/17:00  00/00/00:00
```

   The report indicates that there are three DIG-IP-S (digital IP station) warning alarms:

   - The **Port** field is the port number that is administered to the extension (in the form *SNNNNN*, where *N* is a digit from 0–9, indicating that the port is virtual and a station).
   - The three DIG-IP-S alarms are listed in the **Maintenance Name** field.
   - The **Alt Name** field indicates the administered extension of the IP station.
   - The **Svc State** (Service State) field show that the IP station is in-service.
   - The **Ack?** field indicates that the alarms have not been acknowledged.
   - The **Date Alarmed** field shows the date and time of the alarm.
   - The **Date Resolved** field indicates that none of the alarms have been resolved.

   This example follows the second entry (bold) to resolution.

2. At the SAT type **`display errors`** and press **Enter**.

   The **Error Report** form displays. This form provides similar sort functions as the Alarm report on page 238.

3. Change any fields to narrow your search and press **Enter**.

   The **Hardware Error Report** displays.

```
                    HARDWARE ERROR REPORT - ACTIVE ALARMS

Port      Mtce     Alt      Err   Aux     First        Last      Err Err Rt/ Al Ac
          Name     Name     Type  Data    Occur        Occur     Cnt Rt  Hr  St
S00000    DIG-IP-S 40000    1281  1     09/24/16:43 09/27/15:06 255 3   3   a  n
S00004    DIG-IP-S 40002    1281  1     09/24/16:43 09/27/15:07 255 3   3   a  n
S00009    DIG-IP-S 2553203  1281  1     09/24/16:44 09/27/15:08 255 3   4   a  n
```

This report shows some of the same information contained in the **Alarm Report**, but also indicates that:

- The DIG-IP-S alarm has an **Err Type** (Error Type) of 1281.
- The **Aux Data** (Auxiliary Data) value is **1**.
- The **First Occur** and **Last Occur** fields show when the problem was first logged and the most recent occurrence.
- The **Err Cnt**, **Err Rt**, and **Rt/Hr** fields show the Error Count, Error Rate, and Rate per Hour data, respectively.
- The **Al St** field indicates the alarm state (active).
- The **Ac** field indicates that the alarm has not been acknowledged.

4. Look up the **Mtce Name** (DIG-IP-S, the maintenance object name) in *Maintenance Alarms Reference (03-300430)*.

   Table 58 shows the corresponding information in the Hardware Error Log entries for the DIG-IP-S maintenance object, Error Type 1281, Aux Data of Any. The note (a) below the table tells you what Error Type 1281 means.

Table 58: ETH-PT Error Log Entries

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
1281 (a)	Any	Station Digital Audit test (#17)	WRN	OFF	**test *port* | *station***

Notes:

a. **Error Type 1281** indicates that the terminal is reporting a bad state of health (IP terminal only).

Table 58 and the note indicate that you should run the Station Digital Audit test (#17) to clear the Error Type 1281 (bad state of health in an IP endpoint).

5. At the SAT type **test port *S00004*** (or **test station *40002***) and press **Enter**.

   The **Test Results** appear.

```
test port S00004

                                TEST RESULTS

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

S00004      DIG-IP-S          40002     1372     PASS
S00004      DIG-IP-S          40002     1373     FAIL              1007
S00004      DIG-IP-S          40002     16       PASS
```

The report indicates that 2 tests passed, but test #1373 failed with Error Code 1007.

6. Find Test # 1373 in the DIG-IP-S section and look up Error Code 1007 in *Maintenance Alarms Reference (03-300430)*.

   Table 59 shows the Test #1373 Signaling Path PING Test information for Error Code 1007, Test Result of FAIL:

Table 59: Test #1373 Signaling Path PING Test

Error Code	Test Result	Description / Recommendation
1007	FAIL	The system could not PING the registered endpoint via the CLAN. 1. Verify that at least one destination is reachable through this port. PING this destination (**`ping ip-address`** ***`xxx.xxx.xxx.xxx`***). 2. If a PING to any destination is successful through this port, the link is up. 3. If a PING to every destination fails, test the CLAN port (**`test port`** ***`location`*** **`short`**), and follow repair procedures for Session Status test (#1286) failures. 4. If only this station cannot be pinged: • Make sure the PC is up. • Make sure the PC has a network connection (Ethernet or dial-up). • Check the Ethernet cabling.

5. Perform the repair steps listed in the **Description / Recommendation** column.
6. If the repair steps do not fix the problem, escalate to your technical support representative.

Chapter 6: Troubleshooting IP telephony

- Troubleshooting the TN2302AP and TN799DP circuit packs
- Troubleshooting H.323 trunks
- Troubleshooting problems with shuffling and hairpinning
  - Reviewing a station's IP connection status
  - Reviewing a trunk's IP connection status
  - Reviewing the IP network region status
  - Displaying failed IP network region connections
  - Testing failed IP network regions
  - Conditions and solutions
- Troubleshooting Avaya IP telephones
- Troubleshooting IP Softphone
- No Dial Tone
- Talk path
- Poor audio quality
- Dropped calls
- Echo

Troubleshooting the TN2302AP and TN799DP circuit packs

If your TN2302AP IP Media Processor or TN799DP CLAN circuit pack is not working, try these basic procedures before contacting Avaya for assistance. The following table lists some common circuit pack error messages returned to the System Access Terminal (SAT) and solutions.

Error Message	Solution
“Invalid board location; please press HELP”	Inspect board location. The entered board location is invalid or does not contain a CLAN (TN799DP) board. Use the **`list configuration`** command to location the TN799DP boards.
“No resource administered for this region”	Enter correct resource type on the **IP-Network Region** form.
“This board is not an administered IP-Interface”	Inspect board location. The entered board location contains a CLAN that has not been administered. Use the **`list ip-interfaces`** ***`clan`*** command to see all administered TN799DP boards.

Troubleshooting H.323 trunks

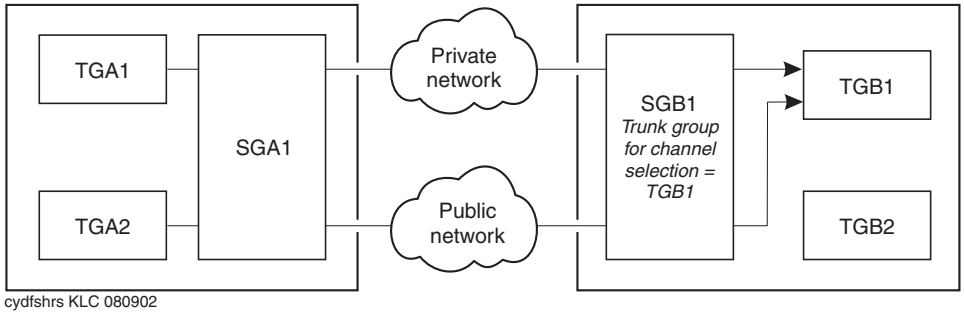
Signaling group assignments

You can assign multiple H.323 trunk groups to a single signaling group. However, when H.323 trunk groups have different attributes, assign each H.323 trunk group to a separate signaling group. An H.323 signaling group directs all incoming calls to a single trunk group, regardless of how many trunk groups are assigned to that signaling group. This is specified in the field **Trunk Group for Channel Selection** on the H.323 signaling group screen.

In the example shown in Figure 34: Shared signaling group on page 251, two trunk groups are assigned to the same signaling group on each of two switches, A and B. Trunk groups A1 and B1 are set up to route calls over a private network, and trunk groups A2 and B2 are set up to route calls over the public network. The signaling group on switch B terminates all incoming calls on trunk group B1 as specified by the **Trunk Group for Channel Selection** field. Calls from switch A to switch B using trunk group A1 and the private network are terminated on trunk group B1, as desired. However, calls from switch A to switch B using trunk group A2 and the

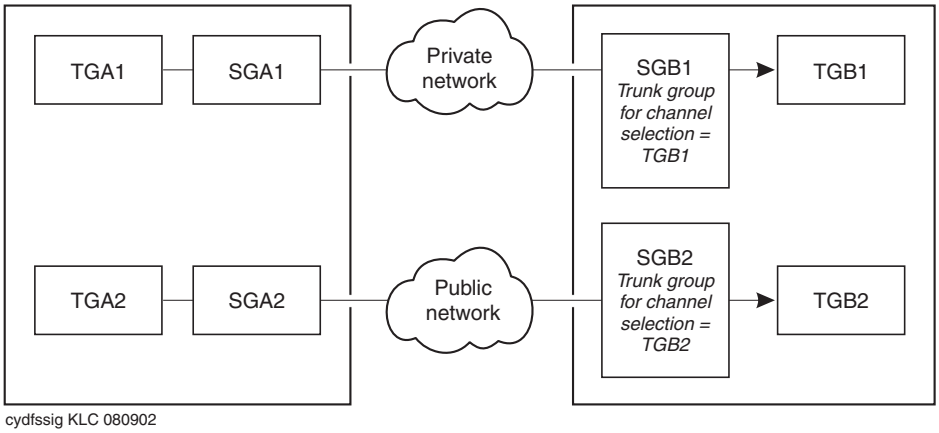
public network are also terminated on trunk group B1, not trunk group B2, which is not the desired outcome.

Figure 34: Shared signaling group



The solution to this problem is to set up a separate signaling group for each trunk group, as shown in Figure 35. More generally, set up a separate signaling group for each set of trunk groups that have *common* attributes.

Figure 35: Separate signaling group



No MedPro resources available

If two switches are connected by an H.323 trunk and all MedPro resources are in use on the call-destination switch when a call is made, the call fails even when a second preference is administered in the routing pattern on the source switch. This can be avoided by setting the first preference Look Ahead Routing (LAR) to **next** in the routing pattern.

CLAN sharing

Depending on the network configuration, a single CLAN board can handle the signaling for multiple applications. For example, the call center Call Management System (CMS) typically uses a small portion of a CLAN's capacity, so the same CLAN can handle the signaling for other IP endpoints at the same time. There are many variables that affect the number of CLAN circuit packs that you need for your network configuration. Contact your Avaya representative to discuss ways to accurately estimate the CLAN resources you need.

Traffic congestion is potentially a problem when multiple IP Interfaces (such as CLAN, IP Media Processor, PCs, CMS) share a network and some of the endpoints are heavily used. This problem can be minimized by using a switched network and assigning endpoints (such as CMS) to a separate LAN/WAN segment.

Troubleshooting problems with shuffling and hairpinning

Shuffling and hairpinning are techniques to more-directly connect two IP endpoints:

- **Shuffling** means rerouting the voice channel connecting two IP endpoints so that the voice exclusively goes through an IP network without using intermediate MedPro resources.
- **Hairpinning** means rerouting a voice channel that connects two IP endpoints so that the voice goes through the MedPro circuit pack in IP format without having to go through the gateway's TDM bus. Only the IP and RTP packet headers are changed as the packet goes through the MedPro. This requires that both endpoints use the same codec.

Use the following procedures to maintain, review, and troubleshoot the status of stations, trunks, and IP network regions:

- Reviewing a station's IP connection status
- Reviewing a trunk's IP connection status
- Reviewing the IP network region status
- Displaying failed IP network region connections
- Testing failed IP network regions
- Conditions and solutions

Shuffling and hairpinning also interact with talk-path problems (see Talk path on page 265).

Reviewing a station's IP connection status

Use the status station command to determine the type of IP connection that is active.

1. Type **`status station`** ***`extension`*** to open the **Call Control Signaling** screen.
2. Move to the AUDIO CHANNEL section of the form.

```
status station 6322                                          Page   x  of   x

                                  AUDIO CHANNEL
                                  Port: S00002
                    Switch                        IP                      IP
                    Port     Other-end IP Addr :Port   Set-end IP  Addr:Port
             Audio:
         Node Name:
    Network Region:
    Audio Connection Type: ip-tdm

                           Port: S00002                Shared Port:
   Product ID and Release: IP_Phone   2.200
  H.245 Tunneled in Q.931? does not apply
      Registration Status: registered-authenticated
              MAC Address: 00:04:0d:4c:1b:2a
       Native NAT Address: not applicable
 ALG - NAT WAN IP address: not applicable
      Authentication Type: DES-56-plus
```

3. Review the following field:

Field	Value
Audio Connection Types	• *ip-tdm* **-** connection is from one endpoint through the TDM bus and back through the Media Processor • *ip-hairpin* **-** connection is between two endpoints that goe through the Media Processor but not through the TDM bus • *ip-direct* - connection goes directly between two endpoints without going through the Media Processor • *ip-idle* - the endpoint is idle and not connected

4. Exit the screen.

Reviewing a trunk's IP connection status

Determine the type of active IP connection.

1. Type **`status trunk`** ***`group/member`*** to open the **Trunk Status** screen.

```
status trunk 1/19
                          TRUNK STATUS

Trunk Group/Member: 01/19                        Service State: in-service/active
              Port: T00123                     Maintenance Busy? no
Signaling Group ID: 1                              CA-TSC state: not allowed
  MM Conference ID: 8
    MM Endpoint ID: 2

Connected Ports: 01B1431 01C1008
                 S00004

            Switch                    IP                      IP
            Port    Near-end IP Addr:Port   Far-end IP Addr:Port
     Q.931:12B1217  xxx.xxx.xxx.xxx: nnnnn  xxx.xxx.xxx.xxx:nnnnn
     H.245:12B1217  xxx.xxx.xxx.xxx: nnnnn  xxx.xxx.xxx.xxx:nnnnn
     Audio:12B1108  xxx.xxx.xxx.xxx: nnnnn  xxx.xxx.xxx.xxx:nnnnn

H.245 Tunneled in Q.931? no
Audio Connection Type: ip-tdm
```

2. Review the following field:

Field	Value
Audio Connection Types	• *ip-tdm* - connections from one endpoint through the TDM bus and back through the Media Processor. For an IP-TDM call, the audio switch port field shows a port on a TN2302AP Media Processor board. • *ip-hairpin* **-** IP connection is between two endpoints and goes through the Media Processor, but not through the TDM bus. For an IP-media processor-IP hairpin call, the audio switch port field shows a cabinet and slot, but not a port, on a TN2302AP Media Processor board. • *ip-direct* - the IP-IP connection goes directly between two endpoints without going through the Media Processor. For an IP-IP direct call, the audio switch port field shows a virtual port number, for example, one starting with "T." • *ip-idle* **-** IP endpoint is idle and not connected. If a trunk is IP-idle, the audio switch port field is blank.

3. Exit the screen.

Reviewing the IP network region status

Use the **status ip-network-region** command to determine if any of the IP network regions failed a ping test. If so, this indicates a connectivity failure between the network region you included in the command and the network region shown on the screen.

1. Type **status ip-network-region *x*** to open the **Inter Network Region Bandwidth Status** screen.

```
status ip-network-region 1                                        Page   1 of 1
               Inter Network Region Bandwidth Status
                                                                          # Times
Src  Dst   Conn    Conn    BW-limits   BU-Used(Kbits)   #-of-Connections  BW-Limit
Rgn  Rgn   Typw    Stat                   Tx      Rx       Tx       Rx    Hit
Today

1      2  direct   pass       NoLimit      0       0        0        0      0
1      3  direct   pass       512:kbits    0       0        0        0      0
1      4  indirect pass                    0       0        0        0      0
1      5  indirect fail                    0       0        0        0      0
1      6  indirect pass                    0       0        0        0      0
1      7  indirect pass                    0       0        0        0      0
1     10  direct   pass       NoLimit      0       0        0        0      0
1     20  direct   pass       NoLimit      0       0        0        0      0
1    100  direct   pass       NoLimit      0       0        0        0      0
1    101  direct   pass       NoLimit      0       0        0        0      0
1    102  direct   pass       NoLimit      0       0        0        0      0
```

2. Review the information on the screen.

   The values indicate that the two regions:

   - **Dst Rgn** not listed - are not administered
   - **fail** - failed the maintenance ping test
   - **pass** - passed the ping test.

3. Exit the screen.

Displaying failed IP network region connections

Use the **display failed-ip-network-region** command to list the 100 network regions with highest number of broken connection paths. If a single network region has a large number of broken paths, the data equipment inside that region is probably the cause of the problem.

1. Type **display failed-ip-network-region** to open the first 100 **Worst Network Regions** report.

```
display failed-ip-network-region                    Page   1 of 1

                    WORST NETWORK REGIONS
      Network Region:Number of Broken Paths

_5:9_    __:__    __:__    __:__    __:__    __:__    __:__    __:__
_4:5_    __:__    __:__    __:__    __:__    __:__    __:__    __:__
_1:2_    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
__:__    __:__    __:__    __:__    __:__    __:__    __:__    __:__
```

   The network regions are ordered from worst to best. For example, in the pictured screen, region 5 has 9 broken paths (5:9) and region 4 has 5 broken paths (4:5).

2. Exit the screen.

Testing failed IP network regions

Use the **test failed-ip-network-region #|*all*** command to initiate a real-time ping test for all failed network-regions connections. If there are no failed network-region connections, the network region connection warning alarm is cleared.

1. Type **test failed-ip-network-region #|*all*** and press **Enter** to begin the test.

   Test results screen appears at end of the test:

```
                          TEST RESULTS

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

        NR-CONN              XXX-YYY     ZZZ         PASS/FAIL/ABORT
```

2. Review the test results.
   - **NR-CONN** represents the Maintenance Object Name for this test.
   - **XXX-YYY** represents the pair of failed network regions being tested.
   - **ZZZ** represents the test number.
   - **Result** will be `PASS`, `FAIL`, or `ABORT`.
   - **Error Code** lists a numeric value in the case of `FAIL` or `ABORT`.
3. Exit the screen.

Conditions and solutions

Consider the following conditions when using hairpinning and shuffling.

Table 60: Considerations with hairpinning and shuffling *1 of 3*

Condition	Solution
Audio Hairpin Connections come undone	The switch may undo hairpinning of audio connections, if a third party is conferenced into the existing two-party call, or when the switch wants to insert a tone or announcement into the connection, or for many other reasons.
Volume is too quiet after a hairpin	An end user using an Avaya endpoint does not have to adjust the volume control, an end-user using a non-Avaya endpoint might need to adjust the audio volume after the audio hairpinning is completed.
Audio Shuffling Connections	The audio shuffling may cause a disruption in the media exchange for a duration of approximately 200ms. The disruption may be longer for an inter-network region call or a call traversing multiple switches. For a call involving an H.323 trunk as one of the endpoints, the administered values of the **Inter-/Intra-region IP-IP Direct Audio** fields on the trunk group associated with that trunk determines the peer PBX's Media Processor capability to handle shuffling: • For a call traversing through multiple switches the shuffling process may continue either leading to a full shuffle or a partial shuffle. • For a normal point-to-point call between two IP terminals the process can begin as soon as the terminating end answers the call. The call may undergo direct ip-ip audio connection or TDM connection based on user actions and feature interactions.
	1 of 3

Table 60: Considerations with hairpinning and shuffling *2 of 3*

Condition	Solution
The yellow LED on Media Processor board remains lit	As long as a TN2302AP Media Processor board is hairpinning calls, its yellow LED is lit. There is no simple way to identify all of the extension numbers that are hairpinning through a particular TN2302AP Media Processor board. It is possible to determine which TN2302AP Media Processor board a particular extension is using for hairpinning by looking at the **Port** field on the **General Status** (`status station`) screen. A hairpinned call will show on this screen as using a TN2302AP Media Processor board slot, but it will not show which TN2302AP port is being used.
TTD equipment is not sending or receiving tones accurately	If Teletype for the Deaf (TTD) equipment is to communicate over H.323 trunks, the system administrator should ensure that G.711 codecs are the primary codec choice for those trunks. This will ensure that the TTD tones are accurately sent through the connection.
Audio quality degrades	Audio quality may suffer if a call is subjected to a series of compressions of different types (some degradation is observed even if the same codec is used multiple times). If hairpinning or shuffling cannot be invoked, then maximum use of a G.711 codec should be encouraged to deal with multiple codec steps.
Switch ends IP audio channel	When an IP-media processor-IP hairpin or IP-IP direct call disconnects, if any set remains off-hook, the switch sends the appropriate tone as administered by the **Station Tone Forward Disconnect** field on the **Feature-Related System Parameters** screen to the off-hook set. • If that administered value is not `silence`, the switch reconnects the audio path of such sets back to a TN2302AP Media Processor port and the TDM bus if an audio channel is available in the same network region. • If that administered value is `silence`, the switch ends the IP audio channel.
Station cannot hairpin	If a station is administered for dual-connect, and if the two extension numbers for that station have differing values administered in their **Inter-/Intra-region IP-IP Direct Audio** fields on the station form, the station cannot hairpin calls.
User experiences one-way audio as soon as the far end connects	If an endpoint is incapable of shuffling and unable to signal that limitation during registration but is administered to allow shuffling, the endpoint user will notice that two-party calls to other IP endpoints that are also capable of shuffling have one-way audio as soon as the far end answers the call. A similar outcome results for calls from such endpoints.
	2 of 3

Table 60: Considerations with hairpinning and shuffling *3 of 3*

Condition	Solution
Service Observer experiences break in speech path	If a call center agent is active on a two-party IP-IP direct call, and a call center supervisor chooses to service observe into the call, the agent would likely notice the 200ms break in the speech path while the call is being shuffled back to an IP-TDM-IP call. Stations that might be service-observed should be administered to block shuffling.
LAN endpoint cannot be administered to allow shuffling	If a LAN endpoint is administered for permanent audio service link operation, the endpoint cannot be administered to shuffle audio connections. Permanent audio service establishes a link that sends a continuous audio stream even when the set is idle and can be used for monitoring.
Calls are dropped during Busyout and Release	Busying out the TN2302AP Media Processor board will drop all calls using the board in any manner. **Note:** Calls carried by IP-IP direct audio connections are not using a TN2302AP Media Processor board. Busying out ports 1-8 on the TN2302AP Media Processor drops all IP-TDM-IP hairpinned calls and prevents such future calls on that port until the port is released, but does not drop IP-media processor-IP hairpinned calls. Busying out a CLAN board causes the sets registered through that CLAN to lose their registrations. If the sets are active on TDM-connected or hairpinned calls, the calls drop. Busying out a CLAN board that is carrying signaling for tandem trunks causes all calls carried over those trunks to drop. What happens to calls carried by direct IP-IP audio connections when the corresponding CLAN board is busied out depends on the endpoints involved in the call. Whether an endpoint drops the call when it loses its registration depends on the type of endpoint. In either case, the switch does not attempt to send new calls to unregistered sets.
	3 of 3

Troubleshooting Avaya IP telephones

If the Avaya IP telephone installation or administration is not working, try these procedures before contacting your technical support representative for assistance. The following table outlines some common IP telephone troubleshooting symptoms.

Symptom	Solution
Unable to access IP Station screens	Make sure the **IP Stations** field on page 4 of the **System Parameters Customer Options** screen is set to **y**. If it is not enabled, you must obtain a new License File.
Port field display on the **Station** screen reads *x*	The field defaults to *x* until a station registers for the first time. After the station has registered once, the **Port** field shows the virtual LAN port address, even if the station unregisters. Use the **list registered-ip-stations** command for a list of registered IP endpoints and their associated ports.
IP telephone not working	Use the **status station *ext#*** command to see if the station is registered. In the AUDIO CHANNEL section the **Registration Status** field should be **registered-authenticated**. To unregister all H.323 endpoints, use the **reset ip-station** command. When the SAT displays *Command completed successfully*, it means that the system has started sending reset messages to all of the H.323 endpoints. After sending the reset messages, the system unregisters the endpoint.

Troubleshooting IP Softphone

Telecommuter use of phone lines

The telecommuter application of the IP Softphone requires the use of two phone lines: one for the IP connection to Communication Manager, which is used for softphone registration and call signaling, and the other for a PSTN connection, which Communication Manager uses as a callback number to establish the voice path. How you allocate your phone lines to these two functions can make a difference.

For example, assume that you have voice mail provided by the local phone company on one of your lines and not the other. In this case, you should use the line with the voice mail to make the initial IP connection to register the Softphone and use the line without voice mail as the POTS callback for the voice path. Otherwise, there could be undesirable interactions between the Softphone and the local voice mail service. For example, if your telecommuter application is registered and you were using your POTS callback line for a personal call when a business associate dialed your work extension, the business associate would hear your home voice mail message.

iClarity audio level adjustments

Note:

This information pertains to the RoadWarrior configuration for IP Softphone.

When your system uses iClarity, and you have trouble hearing the audio on calls, you can use the Avaya IP Softphone Audio Control toolbar and the Audio Status dialog box to check microphone volume and channel power (speakers and headsets) while you are on an active call. You can also use the tools menu to check bandwidth settings and gain. You can run the Tuning Wizard to retrain Avaya iClarity IP Audio to the level of background noise at your location. See your IP Softphone online help for more information.

You can access the Avaya support website at http://support.avaya.com. From there, you can search for additional information, including:

- Recommended Headsets for IP Softphone and IP Agent
- Recommended sound cards for IP Softphone and IP Agent
- USB Headset information
- Avaya IP voice quality Network requirements, including VPN and NAT information

No Dial Tone

Terminology

No dial tone refers to a situation where the light on the IP telephone is on and the display is working, but no dial tone is heard after the IP telephone goes off-hook. No dial tone occurs when

- Connectivity between the MedPro and the IP telephone is interrupted.
- Insufficient DSP resources are available on the MedPro.
- Network Region configurations are incompatibly administered.
- Duplex administration results in a mismatch between the MedPro and the Ethernet switch.

Symptom resolution procedure

To begin diagnosing a no-dial-tone problem, answer the following questions:

1. Has a network assessment ever been done and has the network not been modified after the assessment?

   Y. There may be a network or MedPro problem. All possibilities need to be explored, go to Step 3.

   N. The network may not be compliant with the Avaya's network requirements. If the problem cannot be resolved by using the steps described below, then a (re-)assessment may need to be done, go to Step 2.

2. Look at the large pattern first: do other IP Telephones experience the same problem (assuming multiple IP Telephones are installed)?

   Y. There may be a CLAN, a MedPro, or a network problem. All possibilities need to be explored, go to Step 3.

   N. Go to Step 3 because it could still be that the IP telephone is the only one connected/ registered with the CLAN or only one assigned to the MedPro that has the problem.

3. Because there is a problem with many IP Telephones, is the CLAN that the IP telephone is registered to operational?

   a. Execute the **`status station`** ***`ext#`*** command.

   b. Scroll to the CALL CONTROL SIGNALLING section.

      In the **Switch Port** field look up the slot location of the CLAN circuit pack that is responsible for the IP telephone, for example 07D1703.

   c. Verify that the IP telephone is registered properly with Communication Manager by checking the **Registration Status** field on that page. If the IP telephone is not registered, then ensure that it is registered.

   d. Execute the **`test board`** ***`07D17`*** command.

      This should indicate (all tests should pass) that the CLAN board is operational according to the software. If any test fails then refer to CLAN-BD (Control LAN Circuit Pack) in *Maintenance Alarms Reference (03-300430)*.

   e. Execute the **`status link`** command and ensure that the link is in service.

      If the link is out of service, then check the Installation instructions to make sure the CLAN has been installed and administered correctly.

   If both the **`test board`** and the **`status link`** command do not show any problems with the CLAN board, then go to Step 4.

4. Because there is a problem with many IP Telephones, is the MedPro circuit pack operational?
   a. Go off-hook on the IP telephone.
   b. Execute the **status station *ext#*** command.
   c. Scroll to the CALL CONTROL SIGNALLING section.

      In the Audio Channel section if the **Switch Port** field contains a port location, then go to Step d; otherwise go to Step e.
   d. We have a MedPro port that is dynamically allocated to the IP call. Go to the NETWORK STATUS section and check the **Last Tx Sequence** field that shows the RTP sequence number of the last packet sent by the MedPro to the IP telephone. This sequence number should increase at a regular rate when you run the **status station** command repeatedly. If it does not increase, then there is likely a MedPro hardware or firmware problem. If packets are being transmitted normally, then go to Step 5.

      If the audio channel on the Station form is blank, this might be due to an inability of the MedPro to allocate resource for the call.
   e. Execute the **list measurements ip dsp-resource** command to determine whether there are sufficient MedPro resources in the system.

      Check for denials, blockage and out-of-service condition. If any of those measurements are greater than 0, this may indicate that any of the following problems might exist on the MedPro:

      - The MedPro might have run out of DSP resources. After some users have disconnected, the problem will resolve itself. If this is a regular problem, another MedPro board needs to be installed.
      - The firmware should be FW46 or later. Upgrade the firmware if needed (see Updating software, firmware, and BIOS on page 431 or the Avaya support website http://support.avaya.com).
      - One of the DSPs may be bad or there could be firmware problem. This can be checked in the Hardware Error Log by executing the **display errors** command.
      - Communication Manager might not be able to find a MedPro in the network region where the IP telephone resides.
   f. If there are no MedPro problems, then go to Step 5.
5. Can the MedPro ping the IP telephone?
   a. Execute the **status station *ext#*** command.
   b. Scroll to the CALL CONTROL SIGNALLING section.

      In the **Switch Port** field look up the slot location of the CLAN circuit pack that is responsible for the IP telephone, for example 07D1717.

c. Get the IP address of the IP telephone from the **Set-end IP Addr** field.

Note that hereafter, to simplify the description, it is assumed that this address is 135.9.42.105.

d. Does executing the **ping ip-address *135.9.42.105* board *07D17*** command have a response?

Y. The MedPro receives echo replies from the IP telephone, thus there is network connectivity between the MedPro and the IP telephone. The IP telephone might be faulty. Replace the IP telephone with another one to verify this. If this still does not solve the problem, go to Step 7.

N. The IP telephone is invisible to the MedPro. Go to Step 6.

6. Where did the ping from the MedPro terminate?

a. Execute the **trace-route ip *135.9.42.105* board *07D15*** command.

If network connectivity cannot be established between the MedPro and the IP telephone, one hop will be delineated with "3 *."

b. Begin analyzing the network at the previous router (the last IP address displayed).

7. Are the transmission speed and transmission duplex (HDX, FDX) of the MedPro and the Ethernet switch compatible?

a. Check this by verifying the Layer 1 port statistics on the Ethernet switch connected to the MedPro. Look for Frame check sequence errors, late collisions, and runts.

Y. Go to Step 8.

N. Change the port settings on the Ethernet switch and/or the IP Interfaces form (**change ip-interfaces**) in Communication Manager to make speed and duplex compatible.

Note:

If one side's duplex is set to **autonegotiate**, the other side must also be set to **autonegotiate** or **half**. Locking one side to full duplex will cause errors.

If this resolves the problem then no further steps need to be taken; otherwise go to Step 8.

8. Are the transmission speed and transmission duplex (HDX, FDX) of the IP telephone and the Ethernet switch compatible?

a. Verify the Layer 1 port statistics on the Ethernet switch connected to the IP telephone (frame check sequence errors, late collisions, and runts).

Note:

The switch port *must* be set to **autonegotiate** or **half duplex** or there will be a duplex mismatch.

Y. Go to Step 9.

N. Change the port settings to make speed and mode compatible. If this resolves the problem then no further steps need to be taken, otherwise go to Step 9.

9. There must be a network problem. Compliance with the Avaya network requirements might be an issue as well, and a (re-)assessment may need to be done. Install a protocol analyzer in the network to capture live traffic and analyze the network in further detail.

Talk path

A one-way talk path is a unidirectional voice audio path from one IP telephone to another, that is only one party on a call can hear the other. No-way talk path is the problem where neither party can hear the other, but the call is still connected. Talk path issues often relate to network connectivity issues. Both telephones might have a path to the MedPro, but might not have a route to each other or might be blocked by a firewall. Also, talk-path problems could indicate a shortage of DSP resources on the MedPro. Disabling shuffling is a good way to help diagnose talk-path problems (see also Troubleshooting problems with shuffling and hairpinning on page 252).

Symptom resolution procedure

Three possible problem locations can be identified if users report a one-way or no-way talk path between IP Telephones:

- The network
- The MedPro circuit pack (if the call is not shuffled)
- The IP telephone

For the resolution of this symptom, first disable shuffling (if turned on), which forces traffic to use the media processor, and simplifies the analysis of the network. Then, among other steps, check whether audio/dial-tone can be received by the IP Telephones involved in the call. If necessary, the media processor can check the connectivity of the IP Telephones and their local subnetwork using pings. Layer 1 errors can also be checked.

1. Has a network assessment ever been done and has the network not been modified after the assessment?

   Y. There may be a network problem, a MedPro problem, or the IP telephone may have outdated software. All possibilities need to be explored, go to Step 2.

   N. The network may not be compliant with the Avaya's network requirements. If the problem cannot be resolved by using the procedures described below, a (re-)assessment may need to be done, go to Step 2.

2. Do other IP Telephones on the same VLAN/subnet/floor experience the same problem?

   Y. There may be a network problem, or multiple IP Telephones may have outdated firmware. If the IP telephone firmware version is outdated, download and install the correct firmware (see Updating software, firmware, and BIOS on page 431 or the Avaya support website http://support.avaya.com). If this solves the problem then no further steps are needed, otherwise go to Step 3.

   N. Go to Step 3.

3. Is the call shuffled?

   a. Run the **`status station ext#`** command if a call is in progress.

   b. Scroll to the CALL CONTROL SIGNALLING section.

      If the **Audio Connection Type** field is

      - **ip-direct**, then it is shuffled.
      - **ip-tdm** or **ip-hairpin,** then it is not shuffled.

   Y. If there is no call in progress or the call is ip-direct, turn off shuffling with the **`change station ext#`** command. Set the **Direct IP-IP Audio Connections** field to **n**.

      If this resolves the problem, then there is a network problem that prevents the two IP Telephones from communicating directly. See the note below and go to Step 8.

      If this does not resolve the problem, there could be a network problem or a MedPro problem. Although a network problem is still most likely, keep shuffling disabled and go to Step 4.

   Note:

      The remote PING and remote **`trace-route`** commands can be used to help pinpoint the location in the network where shuffled calls experience problems.

   N. Go to Step 4.

4. Does the IP telephone receive dial-tone?

   Y. Go to Step 5.

   N. Go to the No Dial Tone section.

5. Are there any Communication Manager errors logged for MedPro or the IP telephone?

   a. Run the **`display errors`** command.

      Check the hardware error log and the denial event log for errors against the IP telephone with the particular extension.

   Y. Use the information in the error log and the *Maintenance Alarms Reference (03-300430)* to correct the errors. If this solves the problem, no further steps are needed. Otherwise, go to Step 6.

   N. Go to Step 6.

6. Is voice audio received by the MedPros from both IP Telephones in the call?
   a. Execute the **status station *ext#*** command.
   b. Scroll to the NETWORK STATUS section.

      Look at the **Last Rx/Tx Sequence** field data. These RTP sequence numbers should increase upon repeatedly executing the **status station *ext#*** command.

      Alternatively, Avaya's VoIP Monitoring Manager can be used to verify proper traffic flow.

   Y. Go to Step 4.

   N. The IP telephone is not sending audio or the network is blocking audio packets. Exchange the IP telephone to see if this resolves the problem.

      If this resolves the problem, then replace the IP telephone.

      If it does not resolve the problem, then there is a network problem that the customer needs to resolve.

7. Is the MedPro operating correctly and does it have sufficient MedPro audio resources?
   a. Take an IP telephone off-hook.
   b. Execute the **status station *ext#*** command.
   c. Scroll to the CALL CONTROL SIGNALLING section.

      In the AUDIO CHANNEL section if the **Switch Port** field contains a port location then go to Step d. Otherwise go to Step e.

   d. In this case there is a MedPro port that is dynamically allocated to the IP telephone call. Go to page 5 of the Station form and check the **Last Tx Sequence** field. This field shows the RTP sequence number of the last packet sent by the MedPro to the IP telephone. This sequence number should increase at a regular rate when you run the **status station *ext#*** command repeatedly. If it does not increase, then there is likely a MedPro hardware or firmware problem. Use the *Maintenance Alarms Reference (03-300430)* to resolve the issue. If packets are being transmitted normally, go to Step 8.
   e. If the AUDIO CHANNEL section on the **status station** form is blank, this might be due to an inability of the MedPro to allocate resource for the call. Run the **list measurements ip dsp-resource** command to determine whether there are sufficient MedPro resources in the system. Check for denials, blockage and out-of-service condition. If any of those measurements are greater than 0, this may indicate that any of the following problems may exist on the MedPro:
      - The MedPro may have run out of DSP resources. After some users have disconnected the problem will resolve itself. If this is a regular problem, another MedPro board needs to be installed.
      - The firmware should be FW46 or later. Replace the firmware if needed (see Updating software, firmware, and BIOS on page 431 or the Avaya support website http://support.avaya.com).

- One of the DSPs may be bad or there could be firmware problem. This can be checked in the hardware error log by executing **display errors** command.
- Communication Manager might not be able to find a MedPro in the network region where the IP telephone resides.

If there are no MedPro problems, then go to Step 8.

8. Can the IP telephone that experiences the 1-way problem or both IP Telephones that experience the no-way problem be pinged from the MedPro?
   a. Run the **status station *ext#*** command.
   b. Scroll to the CALL CONTROL SIGNALLING section. The **Switch Port** field gives the slot location of the MedPro circuit pack that is responsible for the IP telephone, for example, 07D1717.
   c. Obtain the IP address of the IP telephone from the **Set-end IP Addr** field. Hereafter, to simplify the description, it is assumed that this address is 135.9.42.105.
   d. Execute the command **ping ip-address 135.9.42.105 board 07D17**.

   Y. The IP Telephones can be pinged from the MedPro, go to Step 10.

   N. The IP Telephones cannot be pinged from the MedPro. Go to Step 9.
9. Find out where the ping terminated.
   a. Execute the **trace-route ip 135.9.42.105 board 07D17** command.

      The customer needs to resolve the network problem in the router that terminated the trace-route command. Go to Step 12 after the problem has been resolved.
10. Is the call going through a firewall/ACLs?
    a. Check if the call would have to traverse a firewall by determining if it is destined to another remote network.

    Y. Relax the packet/port filtering constraints in the firewall if they are too strict. If this works then go to Step 12. Otherwise, go to Step 11.

    N. Go to Step 11.
11. Are there Layer 1 errors detected in the IP telephone, the intermediate switches/ routers or in the MedPro?
    a. Log into the switches and routers using telnet or SNMP access.

       Check the port statistics.

    Note:

    Some customers will not allow this. In such case, the customer should be requested to provide this information.

    Y. There is a network problem (customer responsibility).

    N. Put a Protocol analyzer on both ends of the call by using switch port mirroring to see where packets are being dropped and resolve the problem. Go to Step 12 after the problem has been resolved.

12. If desired, return to the original state again by turning shuffling/hairpinning on if necessary. However, returning to a shuffled state may bring the problem back.
    a. Run the **`change station ext#`** command.
    b. The **Direct IP-IP Audio Connections** and **IP Audio Hairpinning** fields should be set to **y**.

Poor audio quality

Many problems can fall into the category of poor quality audio: clipping of the beginning or ends of words, pops, or crackles.

Poor quality audio is generally caused by network problems. In particular, these problems indicate packet loss on the data network. Common solutions for such problems include applying or tuning QoS parameters and checking for duplex mismatch issues.

This section uses the following terms:

- **Choppy voice**. A voice audio signal that is impaired.
- **Clipping**. Missing pieces in the received voice signal, especially at the beginning or ending of words.
- **Pops**. Sudden interruptions of the voice by a popping sound.
- **Crackles**. Intermittent samples of noise and silence.

All these phenomena could be caused by packet loss or excessive jitter (perceived as packet loss).

Symptom resolution procedure

Several kinds of calls can be distinguished:

- IP telephone - LAN - IP telephone
- IP telephone - LAN - PBX - DCP Telephone
- IP telephone - LAN - PBX - central office - telephone

1. Has a network assessment ever been done and has the network remained unchanged after the assessment?

   Y. There might be a MedPro, IP telephone or network problem, or the IP telephone might have outdated software. All possibilities need to be explored, go to Step 2.

   N. The network may not be compliant with the Avaya's network requirements. If the problem cannot be resolved by using the procedures described below, an assessment or reassessment might need to be done, go to Step 2.

2. Look at the large pattern first: do other IP Telephones on the same VLAN/subnet/floor experience the same problem?

   Y. There may be a network problem, or multiple IP Telephones may have outdated firmware (see Updating software, firmware, and BIOS on page 431 or the Avaya support website http://support.avaya.com). All possibilities need to be explored, go to Step 3.

   N. Go to Step 3.

3. Is a separate VLAN or subnetwork used for voice?

   a. The customer should check this on the Ethernet switches.

      Y. Go to Step 5.

      N. Go to Step 4.

4. Is the number of broadcast messages lower than 1,000 messages per second (this is the number that can safely be handled by the IP telephone)?

   a. Check this by using the network management system or by hooking up a protocol analyzer to the network. If this cannot be checked through the network management system, go to the subsequent steps first, as it takes a relatively large effort to hook up a protocol analyzer.

      Y. Go to Step 5.

      N. There is a network problem. The customer should put the voice traffic (audio and signaling) on a separate VLAN with 802.1p priority 6 (the priority value reserved for voice and other real-time traffic).

5. Is the Ethernet switch connected to the MedPro set to auto-negotiation?

   a. Use the **change ip-interface *location*** command to check the ETHERNET OPTIONS settings.

```
change ip-interface 01A04                                    Page   1 of   1

                                  IP INTERFACES



                 Type: MEDPRO                          ETHERNET OPTIONS
                 Slot: 01A04                             Auto? n
          Code/Suffix: TN2302                           Speed: 100Mbps
            Node Name: mc_medpro1                      Duplex: Half
           IP Address: 135.122.47 .149
          Subnet Mask: 255.255.255.240
      Gateway Address: 135.122.47 .158
  Enable Ethernet Port? y
        Network Region: 1
                 VLAN: n
```

b. Is **Auto** field to **y** (auto-negotiation enabled)?

Y. Go to Step 6.

N. Change the **Auto** field to **y** (auto-negotiation enabled). If this is not possible, set the MedPro speed and duplex to match the switch port.

6. Is the Ethernet switch connected to the IP telephone transmitting in HDX mode?

a. Log in to the Ethernet switch.

The 4606, 4612, 4624, and 4630 IP Telephones are only capable of HDX transmission. The 4602 and 4620 IP Telephones do support full-duplex mode, but require that the Ethernet switch to which they are connected be set to **autonegotiate** mode.

Y. Go to Step 7.

N. Change the switch setting to **HDX** (or **auto** for the 4602 or 4620). If this solves the problem, no further steps need to be taken. Otherwise, go to Step 7.

7. Are 802.1p QoS and IP DiffServ properly and consistently used in the switches, routers, the MedPro and the CLAN?

Check that the QoS usage is consistent by examining the following:

a. At an IP telephone press the keypad button sequence **Hold Q O S #** and use the **#** key to walk through the menu to verify if the following recommended values are used for traffic priorities:

- Layer 2 Audio (802.1p) value = **6**.
- Layer 3 Audio DSCP value = **40** or **46**.
- Layer 3 Signaling DSCP value = **40** or **46**.

b. In Communication Manager execute **`status station`** ***`ext#`*** to determine the CLAN circuit pack to which the IP telephone is registered.

c. Run the **`display ip-interfaces`** command to find the network region for that CLAN circuit pack.

d. Run the **`display ip-network-region`** command to check the QoS settings for the region.

e. Check QoS and IP DiffServ settings in the switches and routers.

Y. Go to Step 8.

N. Turn 802.1p QoS and IP DiffServ tagging on with consistent values across the network by provisioning the recommended values in the switches, routers and IP Telephones. No further steps need to be taken if this solves the problem. Otherwise, go to Step 8.

- Does the call traverse a WAN link? Does it have sufficient bandwidth and QoS/ packet fragmentation?

f. Log on to the WAN routers and verify if the available bandwidth is sufficient to support voice.

Note:

Avaya recommends using G.729, which requires 24 Kbps (uncompressed, excluding Layer 2 overhead). IP packet fragmentation should be turned on when no DiffServ QoS facilities are available. On Avaya and Cisco routers it is possible to minimize bandwidth for audio usage by using the CRTP (compressed RTP).

Y. Escalate the problem to your technical support representative.

N. Go to Step 9.

8. Is the voice codec set to G.729 for calls across a WAN?

   a. This can be checked with an active call going on by running the **`status station ext#`** command.

   b. Scroll to the CALL CONTROL SIGNALLING section.

      In the Audio Channel section it should indicate **G.729** as the encoder used.

   Y. Go to Step 10.

   N. Change the voice codec to **G.729** (which is a lower bandwidth encoder than G.711, but still provides high quality) by executing the **`change ip-codec-set`** command and by putting **G.729** at the top of the codec list. If this solves the problem, no further steps need to be taken. Otherwise, go to Step 10.

9. Is the end-to-end packet loss less than 1%?

   Packet loss greater than 1% may be perceived as poor voice quality. IP Telephony packet loss can be measured using several different tools:

   - The **`list trace station`** and **`status station`** commands show packet loss experienced by the MedPro.
   - Avaya VoIP Monitoring Manager can measure packet loss experienced by IP Telephones as well as media processors.
   - A protocol analyzer can capture packet streams between endpoints and identify packet loss.

   Y. There is a network problem. The customer should explore the possibility to upgrade to a WAN link with the appropriate bandwidth and quality to ensure that it is compliant with the Avaya network requirements, possibly by establishing a new Service Level Agreement (SLA) with a network service provider. A network assessment or reassessment might need to be done.

   N. There may still be a network problem. Escalate the problem to your technical support representative.

Dropped calls

A dropped call is terminated by a mechanism that is outside of user control. For example, a call might be dropped without anyone hanging up. Dropped calls sometimes indicate a connectivity problem on the signaling channel. Such occurrences can be intermittent, and thus difficult to diagnose. If dropped calls do occur frequently, they can be diagnosed using **`list trace station`** or by checking the denial event log.

Symptom resolution procedure

To resolve dropped call problems:

1. Does reconnecting the call solve the problem?

   Y. There may have been an intermittent network problem. No further actions need to be taken unless this happens frequently. In the latter case, go to Step 2.

   N. Install the latest software/firmware on the IP telephone. Download the latest firmware from http://www.avaya.com/support and install it on your TFTP server (see also Updating software, firmware, and BIOS on page 431). To transfer the software to the phone, type **Hold-R-E-S-E-T-#** on the phone. This reboots the IP telephone and downloads a new version from the tftp server. If this resolves the problem, then no further steps need to be taken; otherwise go to Step 2.

2. Has a network assessment ever been done and has the network not been modified after the assessment?

   Y. There may be a network problem, a MedPro problem or a CLAN problem. All possibilities need to be explored, go to Step 1.

   N. The network may not be compliant with the Avaya's network requirements. If the problem cannot be resolved by using the steps described below, a (re-)assessment may need to be done, go to Step 3.

3. Look at the large pattern first: do other IP Telephones experience the same problem?

   Y. There may be a network problem, a MedPro problem, or a CLAN problem. All possibilities need to be explored, go to Step 4.

   N. Go to Step 4.

4. Perform traditional troubleshooting to determine whether Communication Manager or the IP telephone drops the call. For example, this can be done by:

   - Executing the **`list trace station`** ***`ext#`*** command.
   - Checking the denial event log (**`display events`** command, **Category** field = **denial**).

   If this does not solve the problem, then there is a network problem. Compliance with the Avaya network requirements may be an issue as well, and an assessment or a reassessment may need to be done.

Echo

A voice signal that is reflected back to the speaker at an audible level so that it interferes with the ability to have a normal conversation with another party is called echo. In recent years, echo has mostly been imperceptible in circuit-switched networks due to their low delay and the deployment of echo cancellers. IP calls can experience a much larger delay, and therefore echo can be much more noticeable.

Echo can be created in two ways:

- Acoustically, in a telephone handset, a telephone that is operating in speakerphone mode, a speakerphone, a headset, or a multimedia laptop computer or desktop computer with a headset or an integrated or separate microphone and speaker. In particular, speakerphones or telephones that are operating in speakerphone mode provide a high level of acoustical echo return signal. The level of acoustic echo is determined by the acoustics of the environment (such as wall and ceiling reflection), the degree to which loudspeaker and microphone are directed towards each other, and the directional acoustic characteristics of the microphone.
- Electrically, by impedance mismatches in 2-to-4 wire hybrids on analog line or trunk cards, or electrical cross-talk interference in wires or headset adapters.

In general, the perception of echo is call dependent. The perceived echo problems for calls that are made over a WAN are normally much larger compared with calls that are made over a LAN because of the larger delay in WAN-connected systems.

As echo is not caused by an IP network (although it is exacerbated by delay), so its resolution will not be covered in detail in this document. In general, there are three strategies for dealing with echo:

- Tune the network to reduce delay.
- Deploy echo cancellers.
- Tune the Communication Manager loss plan that is associated with the problem area.

When echo is experienced, the problem is generally resolved at the far-end of the link. For more information, see *Avaya IP Voice Quality Network Requirements*.

Chapter 7: Troubleshooting the S8400 Maintenance Processor Complex (MPC)

This chapter contains the following topics:

- MPC channel traffic
- Detecting the MPC
- Testing the internal LAN
- Testing the MPC through SSH
- Testing HPI

MPC channel traffic

All communication between the server and the MPC are via an internal, dedicated LAN. Three major channels (ports) are used in that LAN for host-to-MPC software communications. The MPC forwards traffic on all other channels between its Services port or modem connections and the host. The three channels are for:

- SSH sessions (logging into the MPC)
- HPI (Hardware Platform Interface) traffic (environment and control traffic)
- NTP (time updates)

The way to determine if the MPC is working is to see if any of these channels is working. If any one is and another is not, then the problem is with the channel that is not working. If none is working, then the problem is with the MPC or the internal LAN.

Detecting the MPC

As an administrator, run the **lspci** command. The result should look something like:

```
craft@server1>: lspci
00:00.0 Host bridge: Intel Corp.: Unknown device 2578 (rev 02)
00:03.0 PCI bridge: Intel Corp.: Unknown device 257b (rev 02)
00:1c.0 PCI bridge: Intel Corp.: Unknown device 25ae (rev 02)
00:1d.0 USB Controller: Intel Corp.: Unknown device 25a9 (rev 02)
```

```
00:1d.1 USB Controller: Intel Corp.: Unknown device 25aa (rev 02)
00:1d.4 System peripheral: Intel Corp.: Unknown device 25ab (rev 02)
00:1d.5 PIC: Intel Corp.: Unknown device 25ac (rev 02)
00:1d.7 USB Controller: Intel Corp.: Unknown device 25ad (rev 02)
00:1e.0 PCI bridge: Intel Corp. 82801BA/CA/DB PCI Bridge (rev 0a)
00:1f.0 ISA bridge: Intel Corp.: Unknown device 25a1 (rev 02)
00:1f.2 IDE interface: Intel Corp.: Unknown device 25a3 (rev 02)
00:1f.3 SMBus: Intel Corp.: Unknown device 25a4 (rev 02)
02:01.0 Ethernet controller: Intel Corp.: Unknown device 1075
03:01.0 Ethernet controller: Intel Corp. 82559ER (rev 10)
04:02.0 VGA compatible controller: ATI Technologies Inc Radeon VE QY
04:03.0 Ethernet controller: Intel Corp.: Unknown device 1076
```

Look for “03:01.0 Ethernet controller: Intel Corp. 82559ER (rev 10)”. The “03” indicates the PCI card that the MPC is plugged into and the 82559 is the NIC on the host side of the internal bus. If that line is missing, replace the MPC.

Testing the internal LAN

MPC diagnostics

The place to start is to test the internal LAN. As user **craft** at a server command line shell on the host, run the **sampdiag -v** command. If you see something similar to the following

```
The SAMP is using the Avaya IP address.
SAMP HWaddress: 00:04:0D:6D:DA:E2
SAMP IPaddress: 192.11.13.2
HOST IPaddress: 192.11.13.1
SSH port: 10022
SSH OK
HPI OK

SAMP OK
```

then everything is configured correctly and working.

The **sampdiag** command tries to fix the internal LAN configuration. If there was a problem in how the host internal LAN was configured, then **sampdiag** might have fixed the problem. After a moment, the HPI process recreates itself and the HPI channel should be working. You can run **sampdiag -v** again and see if HPI is recognized.

There are several things to look for in the response from **sampdiag**.

- The SAMP HWaddress line tells you if the MPC was detected. If no HWaddress was detected, then either the ecs.conf file is incorrect or the MPC is not working.
- If the IP addresses are similar to 10.221.248.1 (or .2), then the host was not configured properly when software was installed or the MPC firmware is not up to date.
- This command tests the HPI and SSH configurations for you. If both are failing, but the IP address is reported, then the server software is probably not administered correctly.
- If **sampdiag** cannot determine the IP address, then there could be a problem with the MPC.
- **HPI failing** indicates the MPC firmware probably is not up to date.

MPC configuration diagnostics

Next, run the **ifconfig eth1** command. The results should look similar to the following:

```
craft@server1> ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:04:0D:6D:DA:E2
          inet addr:192.11.13.1  Bcast:192.11.13.3  Mask:255.255.255.252
          inet6 addr: fe80::204:dff:fe6d:dae2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5463 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3474 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2015584 (1.9 MiB)  TX bytes:575903 (562.4 KiB)
```

The things to look for are:

- The inet addr should be 192.11.13.1.
- Both RX packets and TX packets should be greater than zero. If RX packets is 0, then the MPC is not working properly.

Testing the MPC through SSH

At a **craft** login enter the **sampcmd** command from a command line. If the MPC is working, the first time this is done, you will be asked to add a security key. Answer **yes**. After the MPC and host exchange keys and if everything is working, you will see something like the following:

```
craft@server1> sampcmd


              .
             .M
           .MM        _ _
         .MM  M      | (_)
       .MM    M      | |_ _ __  _   ___  __
     MMM  MMMMMMM   | | | '_ \| | | \ \/ /
   MMM        M      | | | | | | |_| |>  <
 MMMM         M      |_|_|_| |_|\__,_/_/\_\



BusyBox v1.00-pre10 (2005.09.19-07:17+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

This is a Linux banner and prompt from the MPC.

Enter **exit** to log out of the MPC.

If you do not see the above, then run the **sampdiag -v** command.

Testing HPI

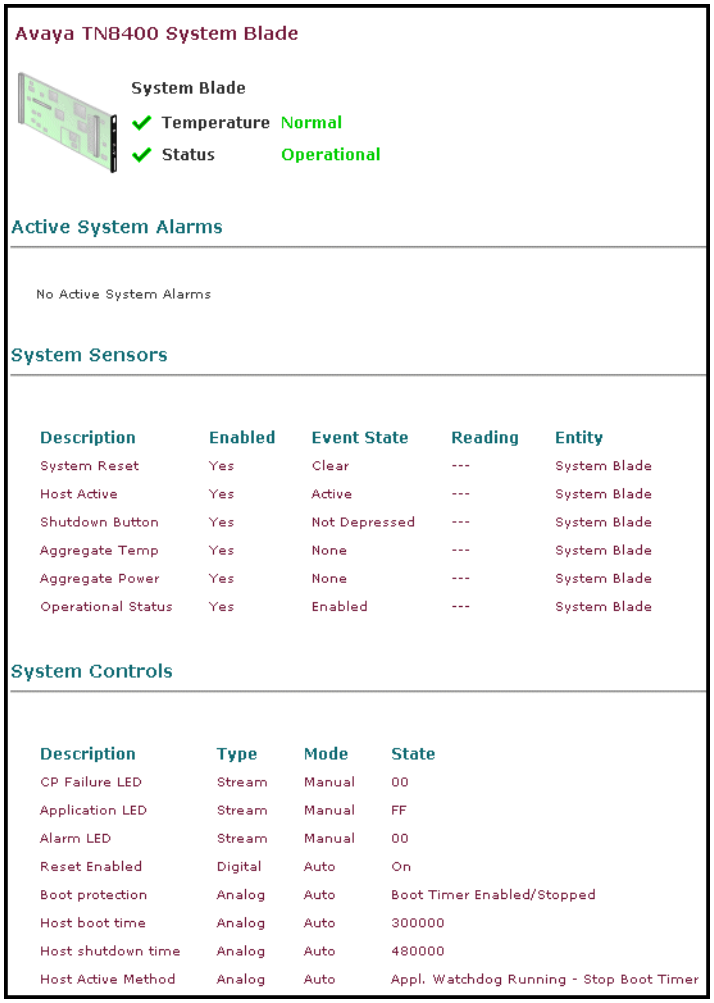
There are several ways to test if the HPI (Hardware Platform Interface) is working, select the one most convenient for your situation:

- As user **craft**, from a command line, enter the **inventory** command. If everything is working, you will see something like

```
craft@server1>: inventory
2       Avaya S8500B    Chassis information     Asset Tag is    5000111222
2       Avaya S8500B    Board Information       Product is      Server Availability Management Card
2       Avaya S8500B    Board Information       Manufactured by Augmentix Corporation
2       Avaya S8500B    Board Information       Product Version is      Avaya S8500B
2       Avaya S8500B    Board Information       Manufactured on 2004-08-13T08:42:29-06:00
2       Avaya S8500B    Board Information       Part Number is  10321 REV.B00
2       Avaya S8500B    Board Information       Serial Number is        STA04310083
2       Avaya S8500B    Board Information       Product Version is      AVAYA_S8500_1_0_SP1_BUILD_11
2       Avaya S8500B    Board Information       Product Version is      INP Firmware AVAYA1 1.18 Mar 2 2005
2       Avaya S8500B    Board Information       Custom is       MAC host 00:0F:29:00:01:5C
2       Avaya S8500B    Board Information       Custom is       MAC eth0 00:0F:29:00:01:5D
```

```
2       Avaya S8500B    Board Information       Custom is       MAC eth1 00:0F:29:00:01:5E
2       Avaya S8500B    Board Information       Custom is       MAC eth2 00:0F:29:00:01:5F
```

- From the MPC Web interface select **Avaya TN8400 System Blade**. If everything is working, you will see a page similar to the following:



- If you do not see anything like the above, log in with administrator privileges to a command line. Enter the **`/opt/desahpi/bin/hpisensors`** command. If everything is working, you should see something like the following:

```
craft@server1>: /opt/desahpi/bin/hpisensors
Opened Session to Domain 1

Resource 306  Avaya S8500B
Sens Num  EvtState       Reading                    IdString
--------  --------  --------------------           --------
     1     0x0001                                  PCI Reset
     2     0x0000                3.344             PCI +3.3V
```

```
   3     0x0007              2.672            PCI +3.3V Aux
   4     0x0000              5.073            PCI +5V
   5     0x0000             11.776            PCI +12V
   6     0x0000            -11.992            PCI -12V
   7     0x0000             12.096            Ext A 12V
   9     0x0000                 35            Samp Temp
  10     0x0001                               Samp +3.3V Fail
  50     0x0002                               Server Power On
  51     0x0001                               System Reset
 101     0x0000            2.59098            MB +2.5V
 102     0x0000            3.33486            MB +3.3V
 103     0x0000             5.0778            MB +5V
 104     0x0000            1.52295            MB +1.5V
 105     0x0000             11.875            MB +12V
 106     0x0000                 34            PCI Area Temp
 107     0x0000                 32            Memory Area Temp
 108     0x0000                 45            CPU Diode Temp
 110     0x0000              10306            Fan Tach 1
 111     0x0000               8655            Fan Tach 2
 112     0x0000               8767            Fan Tach 3
 113     0x0000               8941            Fan Tach 4
 201     0x0000                  0            Alarm Total
 202     0x0000                  0            Alarm Retries
 203     0x0000                  0            Alarms Active
 204     0x0000                               Modem Status
 258     0x0000                               Aggregate Temp
 257     0x0000                               Aggregate Power
 256     0x0000                               Operational Status
```

- Finally, from a command line, run the **`ps -C bridgeip`** command. You should see a response similar to the following:

```
craft@tn8400:~$ ps -C bridgeip
  PID  Uid     VmSize Stat Command
    1 root           SW  [swapper]
    2 root           SW  [keventd]
    3 root           RWN [ksoftirqd_CPU0]
    4 root           SW  [kswapd]
    5 root           SW  [bdflush]
    6 root           SW  [kupdated]
    7 root           SW  [mtdblockd]
   11 root        376 S   init
   17 root           SWN [jffs2_gcd_mtd1]
  166 root        240 S   /usr/sbin/lm90
```

```
  176 root            SW  [khubd]
  364 root        400 S   /sbin/syslogd -m 0 -R my-host:514 -L
  376 root        308 S   /sbin/klogd
  386 root        368 S   /usr/sbin/crond -c /var/cron/crontabs
  532 desahpi     568 S   /opt/desahpi/bin/bridgeipd -v5 -I/opt/desahpi/cmd/bri
  546 desahpi     548 S   /opt/desahpi/bin/bridgeipd -I/opt/desahpi/cmd/bridge2
  547 desahpi     508 S   /opt/desahpi/bin/heartbeatd -I/opt/desahpi/cmd/heartb
  557 desahpi    1624 S   /opt/desahpi/bin/resourced -I/opt/desahpi/cmd/resourc
  566 desahpi     704 S   /opt/desahpi/bin/domaind -I/opt/desahpi/cmd/domain.cm
  615 root        924 S   /opt/alarming/bin/almd --stats
  656 root       1112 S   /usr/sbin/sshd
  670 root        516 S   /usr/sbin/thttpd -C /etc/thttpd.conf
  677 root       1732 S   /usr/sbin/stunnel
  697 root       8736 S   /usr/bin/mdmsvr
  702 root        376 S   /sbin/getty -L tts/0 38400 vt100
  703 root        264 S   /usr/sbin/svcmon
  761 root        336 S   /usr/sbin/mgetty -s 38400 -i /tmp/issue -n 3 -p @\n\r
  788 root       1732 S   /usr/sbin/stunnel
31208 root       1280 S   /usr/sbin/sshd: craft [priv]
31267 craft      1344 R   /usr/sbin/sshd: craft@pts/0
31268 craft       472 S   -sh
  531 root        388 S   sh -c /opt/desahpi/bin/mdmctl
  533 root        396 S   /bin/sh /opt/desahpi/bin/mdmctl
  536 craft       356 R   ps -C bridgeip
  539 root         84 R   [ x = x-d ]  PID TTY          TIME CMD
  317 ?        00:00:00 bridgeip
```

Testing NTP

The MPC updates its date and time from the server once an hour. The date may be off immediately after installation is complete, but should be synchronized after the next MPC reboot or within the hour.

It is difficult to directly test that NTP is working. If the first test (testing SSH) worked, then as user **craft**, run the **sampcmd date** command. You should see something like the following:

```
craft@server1>: sampcmd date
Fri Apr  8 08:19:34 MDT 2005
```

Where the response is the same time and date as the host. If this is not working, then NTP is not set up correctly on the host.

Rebooting the MPC

To reboot the MPC as **craft** login, perform the following step on the host:

- Type **sampcmd sudo reboot** and press **Enter**.

  The MPC then reboots and is unavailable for about a minute.

Chapter 8: Troubleshooting trunks

- Troubleshooting trunks with Automatic Circuit Assurance
- Using Busy Verification of Terminals and Trunks
- Troubleshooting ISDN-PRI
- Troubleshooting ISDN-PRI endpoints (wideband)
- Troubleshooting ISDN-BRI / ASAI
- Troubleshooting ISDN-PRI test calls
- Troubleshooting the outgoing ISDN-testcall command

Troubleshooting trunks with Automatic Circuit Assurance

A display-equipped telephone (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 telephone 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 telephone 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 telephone or attendant console equipped with a “verify” button is required.

Busy Verification of Terminals and Trunks allows a user at a telephone or attendant console to make test calls to trunks, telephones, 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 telephone or resource that is truly busy and one that only appears busy because of a trouble condition.

Troubleshooting ISDN-PRI

Figure 36: Troubleshooting ISDN-PRI (Page 1 of 2) on page 285 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, 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 36: Troubleshooting ISDN-PRI (Page 1 of 2)

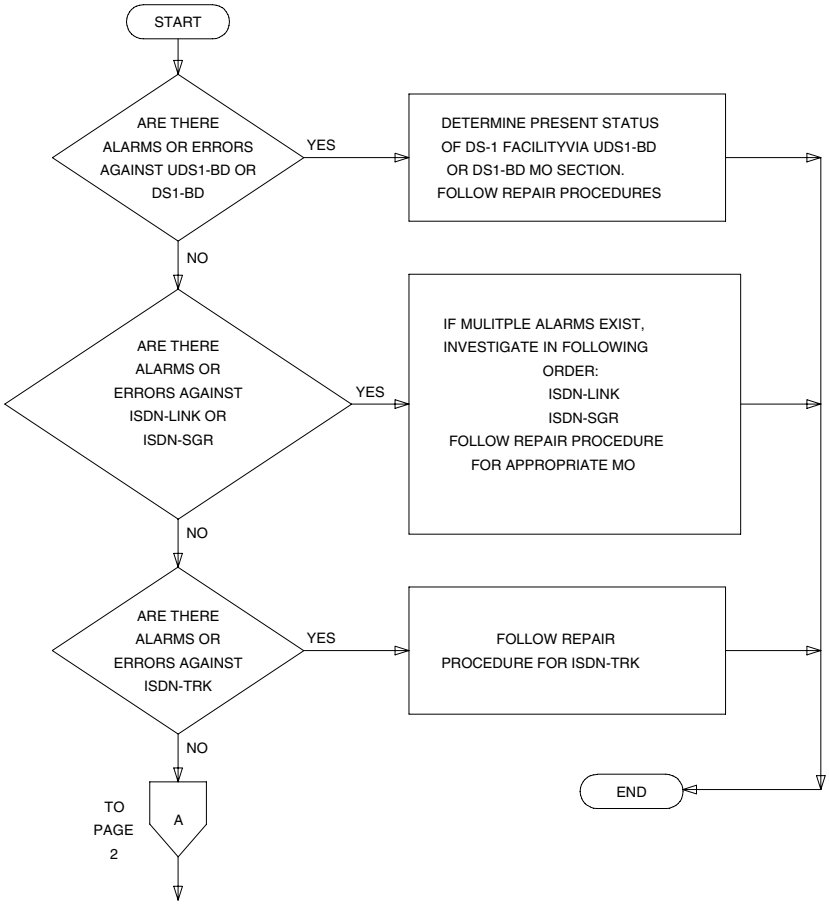
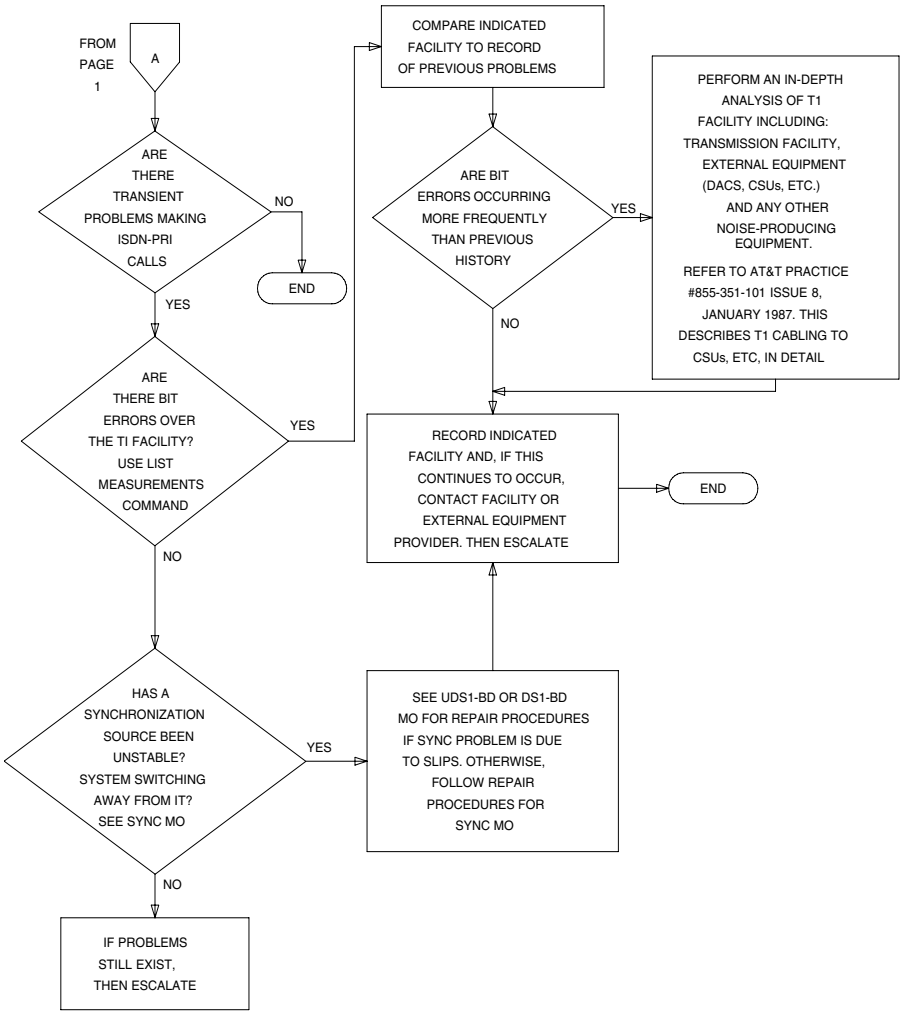


Figure 37: Troubleshooting ISDN-PRI (Page 2 of 2)



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
- PRI endpoint's ports are Layer 3

This troubleshooting procedure is limited to diagnosing faults between the switch and either the ISDN-PRIs:

- 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	YES →	Resolve those alarms or errors in the order listed at left by following procedures for the appropriate MO in *Maintenance Alarms Reference (03-300430)*.
↓ NO		
Check the status of the endpoint equipment or terminal adaptor. (Do this at the endpoint, not at the System Access Terminal-SAT.) ↓		
Does the adaptor or endpoint indicate problems? ↓ NO	YES →	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?	YES →	Correct the administration so that both ends match.
↓ NO		
Does every call fail, or are the failures transient? ↓ Transient Failures	Always Fails →	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.

1 of 2

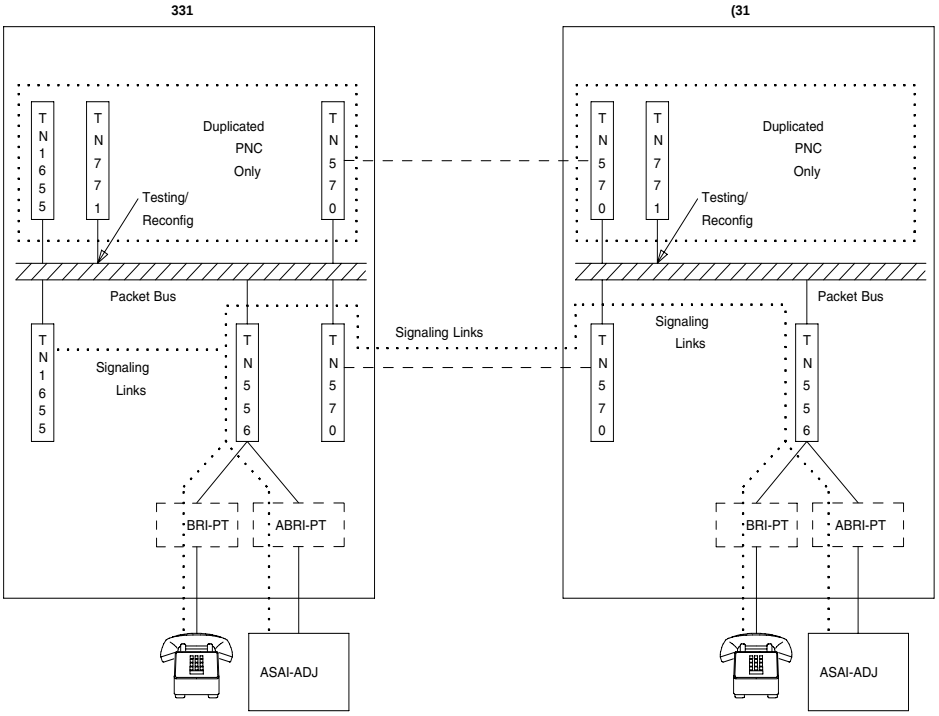
Use **list measurements ds1** to check for bit errors over the **DS1** interface between the switch and the terminal adapter or endpoint equipment. ↓ No bit errors	Bit Errors →	Perform an in-depth analysis of the **DS1** interface including premises distribution wiring, endpoint equipment, and any other 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?	YES →	Follow procedures described in SYNC in *Maintenance Alarms Reference (03-300430).*
↓ NO		
Follow normal escalation procedures.		

2 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 38 shows the connectivity of the packet bus as it applies to ISDN-BRI signaling.

Figure 38: ISDN-BRI/packet-bus connectivity



The flowchart in Figure 39: Troubleshooting ISDN-BRI problems (Page 1 of 2) on page 290 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 commands can also be useful when diagnosing ISDN-BRI problems:

- **status port-network**
- **status packet-interface**

- **status bri-port**
- **status station**
- **status data-module**

Figure 39: Troubleshooting ISDN-BRI problems (Page 1 of 2)

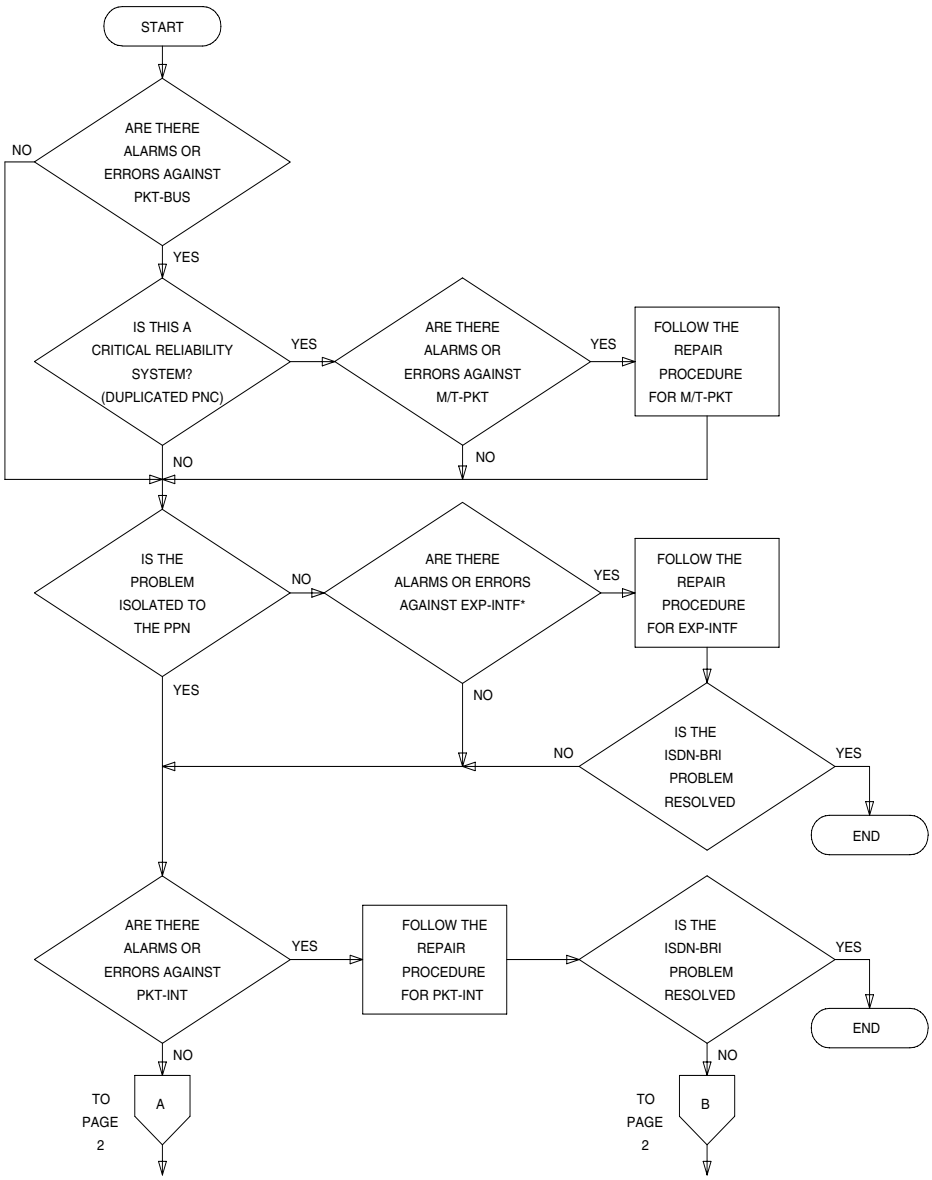
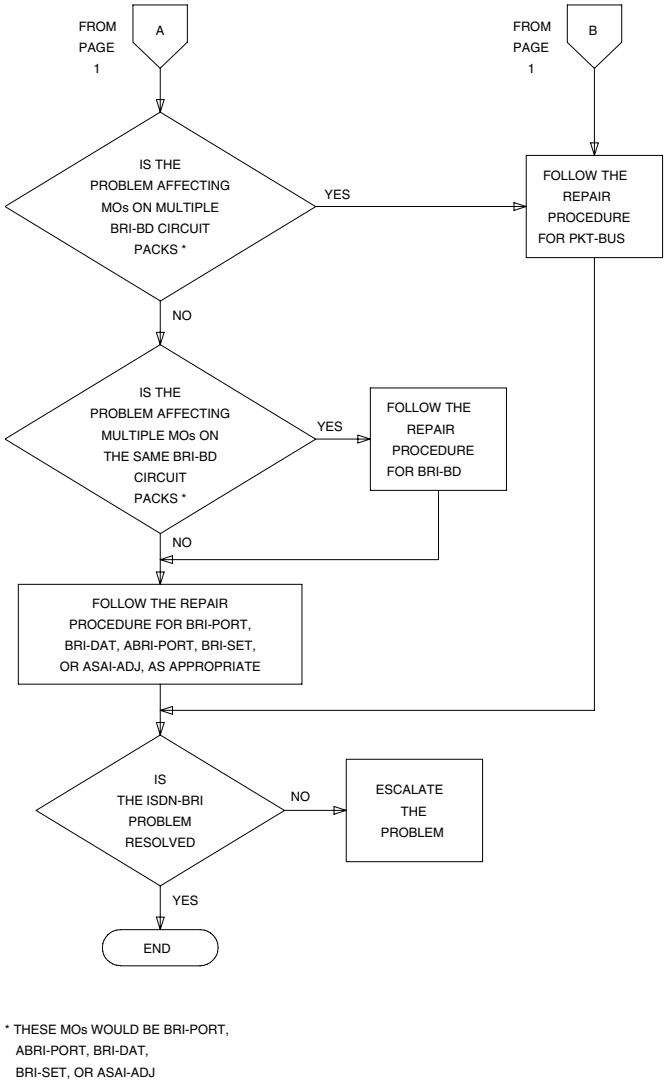


Figure 40: Troubleshooting ISDN-BRI problems (Page 2 of 2)



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 *location* long [repeat#]**
- **test board *location* 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 (***location***) 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, four (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 Feature Access Code (FAC) screen (**display feature-access-code**), 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 41 shows a typical response to the **test isdn-testcall** command:

Figure 41: 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 (***location***) 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 (03-300430)* 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 294.

- **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:

Value	Description
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.

Chapter 9: Other troubleshooting

- Troubleshooting duplicated servers
- Fiber link fault isolation
- Troubleshooting ATM

Troubleshooting duplicated servers

The sections, Server initialization, recovery, and resets on page 125, IPSV-CTL (IP Server 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 an your technical support representative.

CAUTION:

Communication Manager 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.

Note:

The **`display initcauses`** command is not available to customer logins.

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

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	257–769 770, 1281, 1537, 3073, 3074, 3075, 3076, 3585, 3841, 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
2561	15
2817	16
3073	17
3329	18
3585	19
3841	20

- After replacing an SNI circuit pack, clear alarms by executing **`test board`** ***`location`*** **`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 *location* 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 *location* 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 301.

   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 *location* 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 *location* 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 42: Tests for isolating fiber faults on page 302 and Figure 43: DS1 CONV Loopbacks on page 303. Return to Step 4.

If No, did Test #788 fail or abort and Test #789 fail or abort? If yes, execute **test ds1-facility *location* long** command for each administered and equipped DS1 facility.

If No, did Test #797 fail?

If Yes, run the **test ds1-facility *location* 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 43: DS1 CONV Loopbacks on page 303).

- 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.

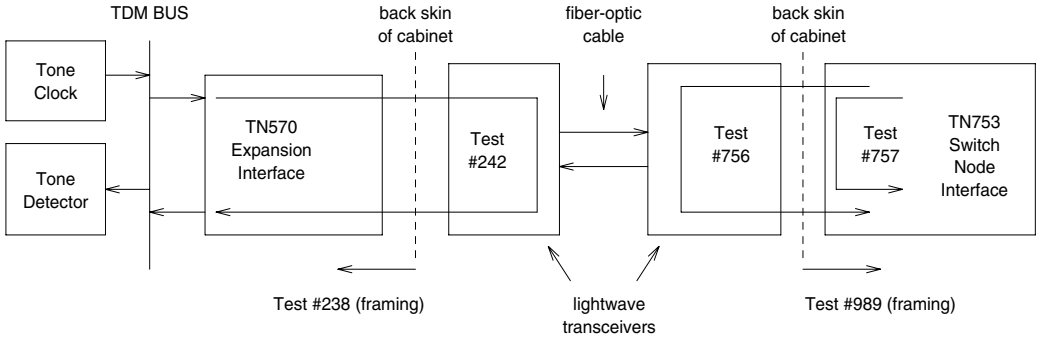
5. At the front of the cabinet, observe the amber LED on the looped back circuit pack.
   - If the amber LED flashes once per second, the circuit pack or transceiver should be replaced.
   - If the amber LED flashes five times per second, the circuit pack or its lightwave transceiver may need replacement. 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 43: DS1 CONV Loopbacks on page 303 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 *location* long** command for an SNI circuit pack.

Test #242 can be run as part of the **test board *location* 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 (03-300430)*.

Figure 42: 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 43: DS1 CONV Loopbacks on page 303. 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 43: DS1 CONV Loopbacks

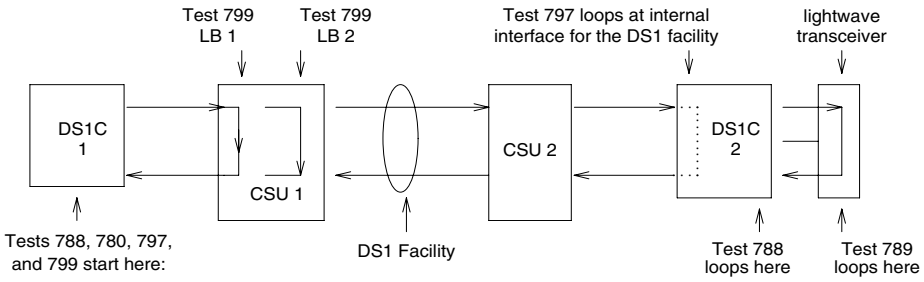


Table 61 shows the pin assignments for the cable used to connect the TN574 DS1 CONV circuit pack to DS1 facilities.

Table 61: DS1 interface cable connectors *1 of 2*

Lead	Desig.	50-pin connector pin number	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

1 of 2

Table 61: DS1 interface cable connectors *2 of 2*

Lead	Desig.	50-pin connector pin number	15-pin connector color	Pin	Color
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
					2 of 2

Troubleshooting ATM

This section provides tips for **S8700 | 8710** ATM PNC when interfacing with the ATM switch. Throughout this section, refer to Figure 44: ATM troubleshooting schematic on page 304.

Figure 44: ATM troubleshooting schematic

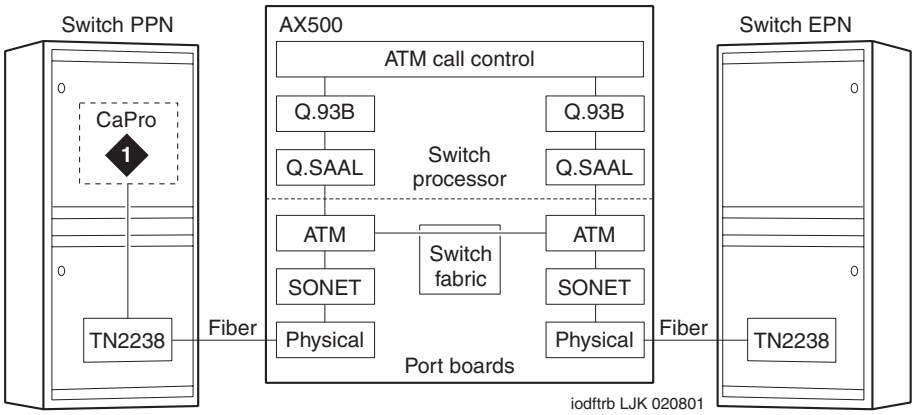


Figure notes:

1 The CaPro element is a software module within the **S8700 | 8710** server.

Initial LED inspection

Visually inspect the LEDs on both the TN230X (Table 62) and the ATM switch (Table 63: A500 LED Quick Reference on page 305) for a high-level status of the system.

Table 62: TN230X LED reference

LED color			Interpretation
Red	**Green**	**Amber**	
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 63 shows the various LEDs on the A500 ATM switch and the meanings of the different states.

Table 63: A500 LED Quick Reference *1 of 3*

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.

1 of 3

Table 63: A500 LED Quick Reference *2 of 3*

Component	Label	Color	State	Meaning
	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.
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	Intermittent 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.

2 of 3

Table 63: A500 LED Quick Reference *3 of 3*

Component	Label	Color	State	Meaning
	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.

3 of 3

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 PNs attached.

- Be aware that customers may use other ports on the A500 for applications unrelated to Communication Manager (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. PNs must be identified by their A500 port numbers.

  Note:

  The following examples show 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 63: A500 LED Quick Reference on page 305)?
- Can you log into the A500 console using the diagnostic account root from the local console terminal or through Telnet? (See Figure 45: A500 login screen on page 308.)

Figure 45: 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:
```

1. Enter **status** at the A500: prompt. Figure 46: A500 screen output for status command on page 308 shows the output from the status command.

Figure 46: 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
```

2. Check for the following conditions and administration:
   - 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.
   - 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?
   - 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?
   - 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?
   - 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** at the S8700 | S8710 SAT. The cabinet, carrier, and slot positions of each administered TN230X board appear as shown in Figure 47. Ensure that each board's physical location matches the display.

Figure 47: 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 *cabinet*** (non-control cabinets) to confirm the PN's board locations and correct insertion.

2. Enter **status pnc**. 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 48 shows the output.

Figure 48: 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 *cabinet*** (for the carrier where the ATM-EI packs reside) or **display circuit-packs *cabinet*** (non-control cabinet). 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 49: Screen output for display circuit-packs 1 on page 311 shows the output for **display circuit-packs *1***. Figure 50: Screen output for display circuit-packs 2 on page 312 shows the output for **display circuit-packs *2***.

Figure 49: 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 50: 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 *portnetwork*** on the S8700 | S8710.

   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 314 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 51 (pnc 1) and Figure 52 (pnc 2).

Figure 51: 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 52: 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 53: Screen output for display atm pnc 1 with End System Identifiers on page 314 (pnc 1) and Figure 54: Screen output for display atm pnc 2 with End System Identifiers on page 314 (pnc 2).

Figure 53: 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 54: 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 55: Screen output for the show signaling summary command on page 315 shows the screen output.

Figure 55: 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
```

2. If an A500 port with an attached 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 If it is User, links will not come up between the PNs.
Signaling	UNI3.1 If it is UNI3.0, links will not come up between the PNs.
ILMI	Preferred value 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 55.)

3. If the A500 was administered using hard-coded PNNI routes to identify each endpoint, enter **show signaling routes** on the A500 console.

   Figure 56: Screen output from the show signaling routes command on page 315 shows the screen output from the command.

Figure 56: 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 on the **S8700 | 8710** server.

4. If the A500 was administered using End System Identifiers, enter **show signaling esi** on the A500 console. Figure 57: Screen output A500: show signaling esi command on page 316 shows the command output.

Figure 57: Screen output A500: show signaling esi command

```
A500:show signaling esi
Addresses registered on A1.1
----------------------------
* 45.0001.01303538105300000000.000000000011.00

Addresses registered on A1.2
----------------------------
* 45.0001.01303538105300000000.000000000012.00

( * - configured )
```

Check that the **Addresses registered** fields (use the **admin signaling esi add** command) match those administered on the **S8700 | 8710** server.

- 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.

5. Enter **show sys interfaces** on the A500 console.

   Figure 58: A500 screen output for show sys interfaces command on page 317 shows the screen output.

Figure 58: 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 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 64: A500: show sys interfaces on page 322.
- **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 either **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 62: TN230X LED reference on page 305) 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*** on the S8700 | S8710 SAT. See the following Figure 59 (carrier 1b) and Figure 60: List configuration carrier 2a screen on page 319 (carrier 2a).

Figure 59: 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 60: 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 378.

4. If the TN230X is inserted and shows a vintage number, enter **test board *location*** for this board on the SAT, as shown in Figure 61 (1b02) and Figure 62: Screen output for the test board 2a01 command on page 320 (2a01).

Figure 61: 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 62: 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

- The TN230X board is in a slot different from the administration.
- 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 296.

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 63 shows the screen output.

Figure 63: 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.

Field	Value
SAP State	`Up` 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 64 shows an example of the screen output.

Figure 64: 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 actions

Perform the following steps to ensure signalling between the ATM board and the ATM switch:

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 65: A500: show stats sonet a1.2 screen on page 324 shows the screen output.

   Note:

   The following examples point to port A1.2 as the port of interest.

Figure 65: 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 field values behave according to these guidelines.

Field	Description
Receive Cell Count Transmit 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.)

- 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.
- If the **Receive Cell Count** field is increasing but the **Transmit Cell Count** field 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 the **Signaling** field is **UNI3.1**.

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.

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?

1. Enter **`show signaling stats port qsaal`** on the A500 console. Figure 66 shows the screen output.

Figure 66: 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.

2. Check the following conditions and administration:

- 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 67 shows the screen output.

Figure 67: 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.

Field	Description
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 Setup Messages 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** might suggest why. The cause code (in following Table 64: Observed cause codes on page 328) 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 68: A500:show signaling cause 31 on page 327 shows the screen output for this command.

Figure 68: A500:show signaling cause 31

```
A500:show signaling cause 31

Cause 31:  Normal, unspecified
```

4. At the S8700 | S8710 SAT type **`display errors`**, and press **Enter**.

   Set the **Error List** to **errors** and **Category** to **PNC** on the input screen, and press **Enter** to display any cause codes (see following Table 64: Observed cause codes on page 328) 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 69 shows the screen output for the **`display errors`** command.

Figure 69: 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 64). 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 64: 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 | S8710 (**`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 | S8710 call volume is too high for the available resources in the ATM network.
63	Service or option unavailable, unspecified	S8700 | S8710 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?

1. Enter **`show switch circuit table`** on the A500 console. Figure 70: A500: show switch circuit table screen on page 329 shows the screen output.

Figure 70: 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 | S8710 call processing.
- Other UBR virtual circuits may exist between A500 ports that are not associated with S8700 | S8710 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 diagnostic steps:

1. Enter **`list sys-link`** on the SAT. Figure 71 shows the screen output.

Figure 71: 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.

Field	Description
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`**. Figure 72 shows the screen output.

Figure 72: 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 Communication Manager and represent the ATM Control Link (ACL) and Expansion Archangel Link (EAL).
- VBRnrt virtual circuits are also be used for ISDN channels between PNs.
- Other VBRnrt virtual circuits may exist between A500 ports that are not associated with 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 table`** on the A500 console. Figure 73 shows the screen output.

Figure 73: 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 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 | 8710**/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 the server and the A500 look good. This section documents some hints and clues that may help diagnose the following failure modes:

- Incorrect PN Route or End System Identifier (A500)
- Swapped Routes, End System Identifiers, or Fiber between a PPN and a PN
- Swapped Routes, End System Identifiers, or Fiber between A- and B-side TN230Xs in a PN
- Swapped Routes, End System Identifiers, or Fiber between two PNs

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

To diagnose talk path conditions:

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 | S8710 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.

Chapter 10: Communication Manager / Linux logs and Tripwire reports

This chapter discusses the information in the many logs that Communication Manager and the Linux platform generate, including some tips for combining and searching the logs. The main topics include:

- Detecting system intrusion
- Accessing system logs through the Web interface
- Interpreting the log entries
- Tripwire

Detecting system intrusion

Some warning signs of system intrusion:

- Unusual login behaviors: perhaps no one can log in, or there is difficulty getting root access; any strangeness with adding or changing passwords.
- System utilities are slower, awkward, or show unexpected results. Some common utilities that might be modified are: **ls**, **find**, **who**, **w**, **last**, **netstat**, **login**, **ps**, and **top**.
- File or directories named "..." or ".." or hacker-looking names like "r00t-something."
- Unexplained bandwidth usage or connections.
- Logs that are missing completely, or missing large sections; a sudden change in syslog behavior.
- Mysterious open ports or processes (**/proc/*/stat | awk '{print $1, $2}'**).
- Files that cannot be deleted or moved. The first thing that an intruder typically does is install a "rootkit," a script or set of scripts that makes modifying the system easy so that the intruder is in control and well-hidden. You can visit http://www.chkrootkit.org and download their rootkit checker.
- Log messages indicating an interface entering "promiscuous" mode, signaling the presence of a "sniffer."

A compromised system will undoubtedly have altered system binaries, and the output of system utilities cannot be trusted. You cannot rely on anything within the system for the truth. Re-installing individual packages might or might not help, since the system libraries or kernel modules could be compromised. There is no way to know with certainty exactly what components have been altered.

Accessing system logs through the Web interface

Note:

If you are using ASG authentication, start the ASG Soft Key application on your laptop computer.

To access the system logs through the Maintenance Web interface to the Linux server:

1. Enter the server IP address in your browser's Address field and press **Enter**.

   The **Integrated Management: Standard Management Solutions** welcome page displays.

2. Click on the **Continue** button.
3. At the notification of a secure connection, Click **OK**.
4. Click **OK** to accept the security certificate.

   The **Integrated Management: Standard Management Solutions** logon page displays.

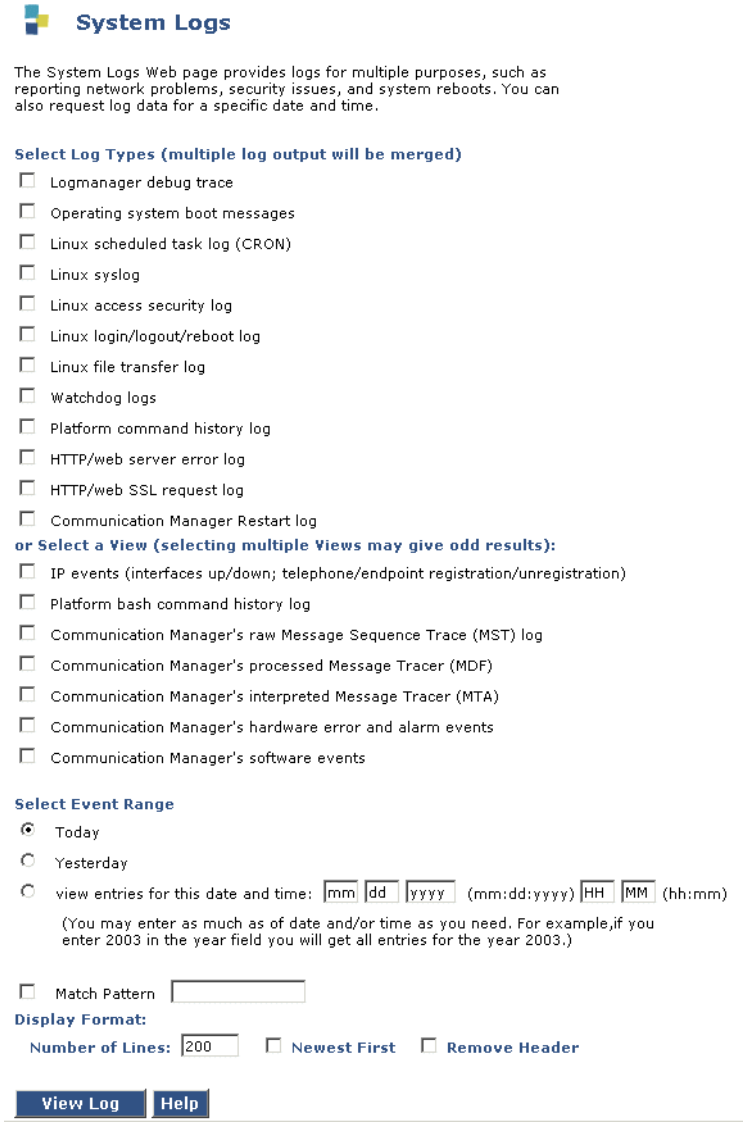
5. Type your login ID (administered login) in the **Logon ID** field.
6. **ASG only**: the **Challenge** field is pre-populated; type this number without the hyphen(s) into the ASG Soft Key application's **Challenge** field. Click on the **Response** button.
7. Leave the **Product ID** field blank (for Avaya use only).
8. **ASG only**: the ASG Soft Key application displays a number the **Response** field; type this number into the **Response** field (OK to use hyphens in this field) on the Web interface and click on the **Logon** button.
9. Answer **Yes** to suppressing alarm origination.
10. The **Integrated Management: Standard Management Solutions** page displays.
11. Click on the **Launch Maintenance Web Interface** link.

    The **Integrated Management: Maintenance Web Pages** license agreement and the navigation pane display.

12. Select **Diagnostics > System Logs** from the left-side navigation pane.

    The System Logs page displays.

Figure 74: System Logs page



Select Log Types

This section of the System Logs page lists several logs and their contents:

- Logmanager debug trace
- Operating system boot messages
- Linux scheduled task log (CRON)
- Linux syslog

- Linux access security log
- Linux login/logout/reboot log
- Linux file transfer log
- Watchdog logs
- Platform command history log
- HTTP/web server error log
- HTTP/web SSL request log
- Communication Manager Restart log

Note:

If you select more than one log, the output is merged and displayed chronologically. If you select the merged log view, you can always tell from which log the entry was written by looking at the log-name field on the entry. This field follows the sequence number field, immediately after the timestamp, and is separated by colons (see also Interpreting the log entries on page 350).

Logmanager debug trace

This log lists:

- All entries contained in the Avaya Communication Manager **`list history`** report.
- IP events: use "IPEVT" in the **Match Pattern** field or select the appropriate view (see IP events on page 347 for more information).
- Auto trace-route commands (a subset of the IPEVT entries)
- Process entries such as restarts, initializations, shutdowns, duplication status, process errors, system alarms, and communication with external gateways and port networks.

Tip:

As an example to restrict/sort the log report type **[action** (use only the left bracket) in the **Match Pattern** field and check the **Match Pattern** box to view the **`list history`**-like entries. Use this for archiving and retrieving **`list history`** legacy reports that are deleted under certain circumstances. Using only “action” in the **Match Pattern** field displays all of **`list history`** entries plus additional debug entries.

To export the log to a separate file you can either:

- Select **View > Source** in your IE browser menu or right-click in the report pane.
- Copy and paste to a text processing application.

Operating system boot messages

This log lists the boot-up processes from the operating system.

Linux scheduled task log (CRON)

This log lists scheduled Linux processes. Use the Web interface to schedule backups (see Backup procedures on page 355 for information about creating scheduled backups.

Note:

Backups and Restores are the only scheduled process that can be initiated from the Web interface.

Figure 75 shows two hourly cleanup cycles from a sample CRON log.

Figure 75: Sample Linux scheduled task log (CRON)

```
20041109:230101000:6084:lxcron:MED:server_name CROND[4375]: (root) CMD (run-parts /etc/
   cron.hourly)
20041109:230001000:6083:lxcron:MED:server_name CROND[4372]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:230000000:6082:lxcron:MED:server_name CROND[4371]: (root) CMD (/opt/ecs/sbin/
   sess_cleanup)
20041109:225000000:6081:lxcron:MED:server_name CROND[1593]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:224000000:6080:lxcron:MED:server_name CROND[31856]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:223000000:6079:lxcron:MED:server_name CROND[29163]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:222000000:6078:lxcron:MED:server_name CROND[26454]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:221000000:6077:lxcron:MED:server_name CROND[24283]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:220100000:6076:lxcron:MED:server_name CROND[21591]: (root) CMD (run-parts /etc/
    cron.hourly)
20041109:220000000:6075:lxcron:MED:server_name CROND[21424]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:220000000:6074:lxcron:MED:server_name CROND[21423]: (root) CMD (/opt/ecs/sbin/
    sess_cleanup)
20041109:215000000:6073:lxcron:MED:server_name CROND[18662]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:214000000:6072:lxcron:MED:server_name CROND[15900]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:213000000:6071:lxcron:MED:server_name CROND[13742]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:212000000:6070:lxcron:MED:server_name CROND[11032]: (root) CMD (/usr/lib/sa/sa1 1
1)
20041109:211000000:6069:lxcron:MED:server_name CROND[8323]: (root) CMD (/usr/lib/sa/sa1 1
1)
```

Linux syslog

This log lists

- Linux process (system) messages
- Server (Linux platform) errors (in an uninterpreted format)

Note:

To view Communication Manager, Linux alarms, and other hardware errors use the **Alarms > Current Alarms** from the Maintenance Web Interface for a clearer view of the application and platform alarms, respectively. Using the Web interface report also identifies which errors require attention.

Communication Manager errors are not logged in the Linux syslog but appear in the Logmanager debug trace log.

- Linux operating system restarts
- Tripwire integrity checks (look for "…twd" entries)
- Disk problems
- Normal events
- Save translations

The Server Maintenance Engine and Global Maintenance Manager processes monitor this log and report alarms.

Linux access security log

This log lists:

- Successful and rejected logins/logoffs from either the Web interface or SAT.

  Note:

  This log does not report access or changes to the Web interface; these appear in the HTTP error log. Any activity at the Web interface appears in this log but not in Communication Manager's list history report.

- At the first incorrect login, the log entry reads "…LOGIN_LOCKOUT…probation interval for login [login] begins," indicating that a timer has started.
  - If the user successfully logs in following a login rejection, the timer expires as indicated by "…LOGIN_LOCKOUT probation interval for [login] ends."
  - If there are 4 incorrect logins within 10 minutes, that login is locked out, indicated by "…login for [login] – failed – user locked out" in the log. To change these parameters, use the information in Table 65: userlock command on page 344.
  - "…failed password check" indicates that the user entered the wrong password.
- Login account is indicated in brackets, for example "[craft]."
- System originating the request.

Figure 76: Sample log: failed Secure Shell SAT loginfc

```
20041110:113254000:2215:lxsec:MED:server_name /usr/bin/sudo: custnsu : TTY=unknown ;
   PWD=/opt/ecs/web/cgi-bin ; USER=root ; COMMAND=/opt/ecs/bin/logc -r -c lxsec today
20041110:113232000:2214:lxsec:MED:server_name PAM_unix_auth[3691]: Login for [custnsu] -
   failed - passwd check
20041110:113232000:2213:lxsec:MED:server_name LOGIN_LOCKOUT[3691]: probation interval for
login
   [custnsu] begins
20041110:113230000:2212:lxsec:MED:server_name PAM_unix_auth[3691]: Login for [custnsu] -
   from [(null)@services-laptop],tty[NODEVssh]
20041110:112621000:2211:lxsec:MED:server_name logmanager: SAT_auth:Logoff for Sid
[0x800e42d]
20041110:112540000:2210:lxsec:MED:server_name logmanager: SAT_auth:Login for [custnsu] Sid
   [0x800e42d] successful
20041110:112540000:2209:lxsec:MED:server_name logmanager: SAT_auth:Login attempt for
[custnsu]
20041110:112538000:2208:lxsec:MED:server_name /usr/bin/sudo: custnsu : TTY=pts/3 ;
   PWD=/var/home/defty ; USER=root ; COMMAND=/opt/ecs/bin/sat -A
20041110:112538000:2207:lxsec:MED:server_name PAM_unix_auth[1426]: secure sat connection
   detected, changing shell to /opt/ecs/bin/autosat
20041110:112538000:2206:lxsec:MED:server_name sshd[1426]: Accepted keyboard-interactive for
   custnsu from 192.11.13.5 port 1265 ssh2
```

What to look for in this log -

- Login entries without "`successful`" are attempts only; use the **Match Pattern** utility at the bottom of the page to search on "`failed`."
- Entries containing "`root`" or "`sroot`" indicate activity at the Linux root level. Ensure that root access is closely monitored:

  ```
  20041109:114051000:4270:lxsys:MED:server_name
  PAM_unix_auth[22971]: Login for [sroot] - successful
  ```

- Tripwire changes appear as "`doenabletrip`," indicating that changes were made to the Tripwire page. Tripwire monitors changes to files that are expected to change, however Communication Manager purposely does not monitor files that routinely change. See Tripwire on page 350 for more information.
- **ASG only**: question any login from an IP address other than that for the ASG Guard:

  ```
  20041109:113504000:4255:lxsys:MED:server_name
  PAM_unix_auth[21826]: Login for [ION] - from
  [(null)@161.127.228.32], tty[NODEVssh]
  ```

Other considerations -

- You cannot set an SNMP trap to monitor login/security violations.

Changing the lockout parameters -

Use the **userlock** command to change the login probation interval and login attempts. This command is issued at the shell only, not the Maintenance Web Interface. Set up shell access by either:

- Telnet or SSH to the standard ports, respectively, and log in.
- At the Communication Manager SAT type **go shell** (must have shell access permissions) and press **Enter**.

The command parameters are listed in Table 65.

Table 65: userlock command

Command	Argument	Use
userlock	**-u *login***	Unlock a locked-out login
	-t *tries*	Sets the number of unsuccessful login attempts before a login becomes locked out (use “inf” for infinite attempts).
	-i *interval*	Minutes before failed login attempts are cleared (“inf” do not clear failed login attempts).
	-o *lockout*	Number of minutes that a login is locked out (“inf” to permanently lock login out).
	-s *show*	Show current parameters and login attempts.

Linux login/logout/reboot log

This log lists:

- Linux logons and logouts
- System reboots

Linux file transfer log

This log lists:

- Information about files copied to or retrieved from the system, including the time, user, and the filenames involved.

Watchdog logs

This log lists:

- Application starts/restarts/failures
- Shutdowns and Linux reboots
- Processor occupancy (excessive CPU cycles)
- SNMP traps started/stopped
- Memory
- Process sanity

Log entries that are system-affecting are reported as alarms. This log does not contain hacking/intrusion information, except for terminating an application.

Platform command history log

This log lists commands that modify the server administration or status, including software updates that have been installed.

Note:

For a log of the shell commands that have been executed, look at the Linux syslog or choose the Platform bash command history view from the System Logs page (see Figure 74: System Logs page on page 339).

Figure 77: Sample platform command history log

```
20041109:220026000:428:cmds:MED:server_name root: filesync trans_lsp
20041109:220017000:427:cmds:MED:server_name logger: fsy_logins
20041109:220009000:426:cmds:MED:server_name root: /opt/ecs/sbin/filesync ipsi
20041109:220008000:425:cmds:MED:server_name root: hostscfg -a -I198.152.254.1 -H
ipsi-A01a:
20041109:220008000:424:cmds:MED:server_name root: hostscfg -d -H ipsi-A01a
20041109:164809000:423:cmds:MED:server_name logger: ip_fw -w
20041109:164756000:422:cmds:MED:server_name logger: ip_fw -w -q
20041109:163019000:421:cmds:MED:server_name logger: ip_fw -w -q
20041109:130604000:420:cmds:MED:server_name logger: ip_fw -w
20041109:130536000:419:cmds:MED:server_name logger: ip_fw -w -q
20041109:105826000:418:cmds:MED:server_name craft: productid
20041109:105526000:417:cmds:MED:server_name logger: ip_fw -w
20041109:105411000:416:cmds:MED:server_name logger: ip_fw -w -q
20041109:105137000:415:cmds:MED:server_name craft: /etc/init.d/iptables status
20041109:102934000:414:cmds:MED:server_name craft: update_show.
20041109:102934000:413:cmds:MED:server_name logger: swversion
```

HTTP/web server error log

This log lists errors and events that are generated by the platform Web server, including:

- Web server restarts
- Abnormal CGI script file terminations
- Certificate mismatches

This log contains more detail (including IP addresses of the server as shown in Figure 78) on activity run from the Web interface (including errors) than the Linux access security log. Also, this log shows all actions taken from the Web interface by listing the programs that are run and their parameters. The program names are the key to understanding the action performed.

Figure 78: Sample HTTP/web error log

```
20041109:105526000:2440:httperr:MED:[error] [client 192.11.13.5] w_dolansec running command:
   /usr/bin/sudo /opt/ecs/sbin/ip_fw -w 2&gt;&amp;1 , referer: https://192.11.13.6/cgi-bin/
   cgi_main?w_lan_sec
20041109:105526000:2439:httperr:MED:[error] [client 192.11.13.5] w_dolansec: calling exec:
   sudo /opt/ecs/web/cgi-bin/w_dolansec2, referer: https://192.11.13.6/cgi-bin/
   cgi_main?w_lan_sec
20041109:105526000:2438:httperr:MED:[error] [client 192.11.13.5] cgi_main: calling exec :
   /opt/ecs/web/cgi-bin/w_dolansec, referer: https://192.11.13.6/cgi-bin/cgi_main?w_lan_sec
20041109:105412000:2437:httperr:MED:[error] [client 192.11.13.5] , referer:
   https://192.11.13.6/cgi-bin/cgi_main?susers_menu
20041109:105412000:2436:httperr:MED:[error] [client 192.11.13.5] w_lan_sec running command:
   /usr/bin/sudo /opt/ecs/sbin/ip_fw -w -q 2&gt;&amp;1 , referer: https://192.11.13.6/
   cgi-bin/cgi_main?susers_menu
20041109:105412000:2435:httperr:MED:[error] [client 192.11.13.5] w_lan_sec: calling exec:
   sudo /opt/ecs/web/cgi-bin/w_lan_sec2, referer: https://192.11.13.6/cgi-bin/
   cgi_main?susers_menu
```

What to look for in this log -

- "...`w_lan_sec2`" indicates access to the firewall page; "...`w_dolansec2`" indicates a change to the firewall settings:

  `20041109:105526000:2440:httperr:MED:[error] [client 192.11.13.5]` **`w_dolansec`** `running command: /usr/bin/sudo/opt/ecs/sbin/ip_fw -w 2>&1 , referer: https://192.11.13.6/cgi-bin/ cgi_main?w_lan_sec`

  `20041109:105412000:2435:httperr:MED:[error] [client 192.11.13.5] w_lan_sec: calling exec: sudo /opt/ecs/web/cgi-bin/`**`w_lan_sec2`**`, referer: https://192.11.13.6/cgi-bin/cgi_main?susers_menu`

- Changes to the system configuration appear in the log as "`w_config`..."

HTTP/web SSL request log

This log lists all requests made of the Web server's SSL module, indicating all requested pages or those placed in secure mode.

Communication Manager Restart log

This log parallels the display initcauses SAT report that shows the active & standby server activity and lists the:

- Last sixteen (16) Communication Manager restarts
- Reason for the request
- Escalation of restart level

Select a View

This section of the System Logs page allows you to select a viewpoint for the data in the various logs. Selecting multiple Views might give odd results.

- IP events
- Platform bash command history log
- Communication Manager's raw Message Sequence Trace (MST)
- Communication Manager's processed Message Tracer (MDF)
- Communication Manager's interpreted Message Tracer (MTA)
- Communication Manager's hardware error and alarm events
- Communication Manager's software events

IP events

This log lists:

- Interfaces (CLAN, MEDPRO, VAL, IP stations) up or down
- Registering/unregistering gateways and IP endpoints
- Reason for IP phone unregistration
- IP address of station registering
- CLAN through which the registration occurred
- Automatic traceroute events

If you want IP events to appear in this log only, you can configure the **list history** command through the SAT interface to omit IP events. The **list history** log can hold up to 1,500 entries, and configurations with IP endpoints can fill this log quickly. Alternatively, you can send all IP event information to the IP events log, which has a greater capacity than the **list history** log.

Figure 79: Sample IP event log

```
20041109:131342365:34112:capro(20388):MED:[ IPEVT    IPT_REG board=01A07 ip= 161.127.228.23
   net_reg=   1  ext=  24100 ip= 161.127.228.47: 3000 net_reg=   1 reason=normal]
20041109:130224805:34083:capro(20388):MED:[ IPEVT    IPT_REG board=01B07 ip= 161.127.228.21
   net_reg=   1  ext=  24101 ip= 161.127.228.27:49300 net_reg=   1 reason=normal]
20041109:112805025:33726:capro(20388):MED:[ IPEVT  IPT_UNREG board=01A07 ip= 161.127.228.23
   net_reg=   1  ext=  24101 ip= 161.127.228.27:49300 net_reg=   1 reason=2010]
```

The final entry in Figure 79 lists a reason code of 2020, which exactly matches the Denial Event entry that is logged in the Communication Manager denial event log (**display events** and type **denial** in the **Category** field of the **Event Report** form). See *Maintenance Alarms Reference* (03-300430) for more information about denial events.

Platform bash command history log

This log lists all commands that have been issued from the server's command line interface for the last month.

Some acronyms that appear in this log are:

- PPID = parent process ID
- PID = process ID of shell
- UID = is a number that the system associates with a login, for example, "0" is root; all other numbers match to login names.

Figure 80: Sample bash history log

```
20041109:165606000:4426:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778
20041109:164626000:4420:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 more sar01
20041109:164623000:4419:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 file sar01
20041109:164616000:4418:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 man sal
20041109:164613000:4417:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 man sa
20041109:164603000:4416:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 file sa01
20041109:164549000:4415:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 ls -l
20041109:164548000:4414:lxsys:MED:server_name bash: HISTORY: PPID=3266 PID=539 UID=778 ls
```

Communication Manager's raw Message Sequence Trace (MST)

For use by Avaya technical service representatives.

Communication Manager's processed Message Tracer (MDF)

For use by Avaya technical service representatives.

Communication Manager's interpreted Message Tracer (MTA)

For use by Avaya technical service representatives.

Communication Manager's hardware error and alarm events

This log lists the same items that report as **`display alarms`** (SAT) or **Alarms > Current Alarms** (Web interface) only in log format.

Communication Manager's software events

For use by Avaya technical service representatives.

Select Event Range

Use this section of the **Diagnostics > System Logs** page to refine/restrict the log report:

- **Today** displays log entries for the current date.
- **Yesterday** displays log entries for the previous day.
- **View entries for this date and time** allows you to specify a date and/or time range. Use any or all of the fields to refine your search. For example, if you wanted to view the current month's activity, type the 2-digit month in the **MM** field (1st field) only. If you want to view entries for the last hour, type the 2-digit hour in the **HH** (2nd field).
- **Match Pattern** allows you to search for log entries containing the search string that you type into this field.

Display Format

- **Number of Lines** restricts the log report to a specified number of entries (1-100,000)
- **Newest First** lists the most recent log entries first.
- **Remove Header** removes the sequence number, the log process, and the priority fields from the log entries. This reduces the line length of each entry for easier viewing.

1. Click on the **View Log** button to view the log report.

Interpreting the log entries

Each line of the log consists of common information, followed by log-specific information. The beginning of each line contains information, separated by colons (:), and looks similar to the following:

```
20030227:000411863:46766:MAP(11111):MED:
```

If you select the merged log view, you can always tell from which log the entry was written by looking at the log-name field on the entry. This field follows the sequence number field, immediately after the timestamp, and is separated by colons.

Interpret the information as follows:

- **20030227** is the date (February 27, 2003)
- **000411863** is the time (00 hours, 04 minutes, 11 seconds, 863 milliseconds (ms) or 00:04:11 AM).
- **46766** is the sequence number of this entry.
- **MAP(11111)**, an example from the Logmanager debug trace on page 340 is the name and number of the process generating the event. Other logs display as an abbreviated name, for example "lxsys" for the Linux syslog and "httperr" for the HTTP/web server error log.
- **MED** is the priority level (medium).

Following the generic information the log-specific information appears in brackets [].

Tripwire

Tripwire is a host-based intrusion detection system that monitors the filesystem for changes. Based on the presumption that an intruder who gains root access would probably make changes to the system somewhere. Tripwire utilities can

- Monitor the various aspects of the filesystem.
- Compare them against a stored database.
- Alert the user if any changes are detected.

Tripwire monitors file integrity by maintaining a database of cryptographic signatures for programs and configuration files installed on the system, and reports changes in any of these. A database of checksums and other characteristics for the files listed in the configuration file is created. Each subsequent run compares any differences to the reference database, and the administrator is notified. The greatest level of assurance that can be provided occurs when Tripwire is run immediately after Linux has been installed and security updates applied, and before it is connected to a network. A text configuration file, called a policy file, defines the

characteristics for each tracked file. Administration requires constant attention to the system changes and can be time-consuming if used for many systems.

The Tripwire report lists modifications to files that it monitors and compares to its database. Tripwire monitors changes to files that are *expected* to change, however Communication Manager purposely excludes files that routinely change from Tripwire monitoring.

Topics discussed in this section include:

- Enabling Tripwire
- Tripwire Commands

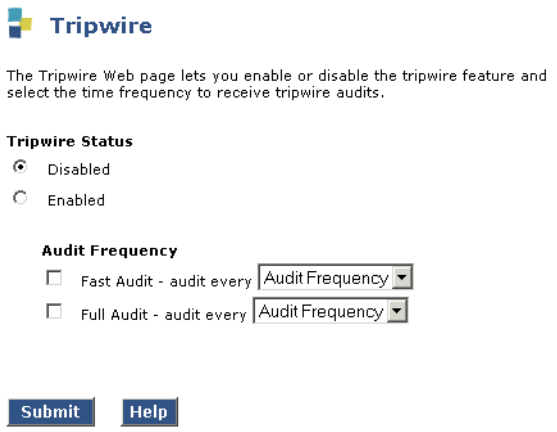
Enabling Tripwire

To enable Tripwire and set the audit frequency from the Web interface:

1. From the left-side navigation pane, select **Security > Tripwire**.

   The **Tripwire** page displays.

Figure 81: Tripwire page



2. **Tripwire Status**: select the Enabled button. If a signature database does not exist, another page prompts you to add a Tripwire database. To add the database click **Yes**; if you select **No**, a page appears indicating that Tripwire is disabled and a signature database is not created.
3. **Audit Frequency**: choose from

   Fast Audit

   - 15 minutes
   - 30 minutes
   - 1 hour

- 2 hours
- 4 hours
- 8 hours
- 12 hours

Fast audits are created in the /etc/cron.d. file. Audits that run at 15- and 30-minute intervals are started on the quarter-hour and half-hour, respectively. The audit does not begin immediately but starts at the next time interval specified. Hourly audits begin at 3 minutes past the hour.

Full Audit

- hourly
- daily
- weekly

Full audits are created in the /etc/cron.daily, /etc/cron.hourly, or /etc/cron.weekly files, depending on the frequency selected.

4. Click on the **Submit** button.

Tripwire Commands

After you have enabled Tripwire:

1. Select **Security > Tripwire Commands** from the left-side navigation pane of the Web interface.

   The **Tripwire Commands** page displays.

Figure 82: Tripwire Commands page

2. Select **View tripwire report** and click on the **Submit** button.

   The **View Tripwire Logs** page displays all of the available Tripwire logs. The file names have the date and time with a file extension of ".trw."

3. Select the log by clicking the radio button to the left of the file name.

   The **View Tripwire Logs Results** page displays.

Figure 83: Sample Tripwire log

```
================================================================================
Rule Summary:
================================================================================

--------------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  Linux Temporary Directories     20                0        0        0
  Linux System                    300               0        0        0
  Fast Audit                      300               0        0        0
* Linux Config Files              300               0        0        1
  MV Config Files                 20                0        0        0
  Var Files                       300               0        0        0
* Root Config Files               300               2        0        0
  Critical Devices                300               0        0        0
  Critical System Boot Files      300               0        0        0
* MultiVantage Files              300               3        0        1

Total objects scanned:  17499
Total violations found:  7
```

4. Look in the “Rule Summary” section for **Total Violations Found**, a number that indicates the total combined changes to the “Rule Name” list.

   Note:

   “MultiVantage Files” means Avaya Communication Manager files.

Reclaiming a compromised system

Unfortunately, there is no way to find with assurance all of the modified files and backdoors that might have been left without a complete re-install. Trying to patch up a compromised system risks a false sense of security and might actually aggravate an already bad situation.

To reclaim a compromised system:

1. Power down the server and disconnect it from the network.
2. Back up Communication Manager translation, but *do not* include any system files or system configuration files in the backup (see Backup procedures on page 355). Translation are safe to back up because they contain internal consistency checking mechanisms.
3. Reformat the drive before re-installing software to ensure that no compromised remnants are hiding. Replacing the hard drive is a good idea, especially if you want to keep the compromised data for further analysis.
4. Re-install Communication Manager (30+ minutes).

   Note:

   The best time to install Tripwire or another intrusion detection system is after a clean install.
5. Reconfigure the server using the Web configuration wizard or the Avaya Installation Wizard (AIW). This takes 30+ minutes.
6. Apply all software updates as appropriate.
7. Restore the Communication Manager translations (see View/Restore Data on page 369).
8. Re-examine your system for unnecessary services (**`/proc/*/stat | awk '{print $1, $2}'`**).
9. Re-examine your firewall and access policies.
10. Create and use new passwords.
11. Re-connect the system to the network.

Chapter 11: Backup procedures

This chapter contains information about backing up the various file sets that are associated with your Avaya media server using the Maintenance Web pages:

- S8500 and S8700 backup procedures
- S8300 backup procedures

Additionally, the following sections discuss the other backup and restore options:

- Backup History
- Schedule Backup
- Backup Logs
- View/Restore Data
- Restore History
- Format PC Card

S8500 and S8700 backup procedures

Tip:
If you backup using file transfer protocol (FTP) or Secure Copy (SCP), you will need the following information to complete the procedure:

- User name
- Password
- Host Name
- Directory (path)

This procedure backs up data files for the Avaya S8500 and S8700 media servers using the Maintenance Web Pages:

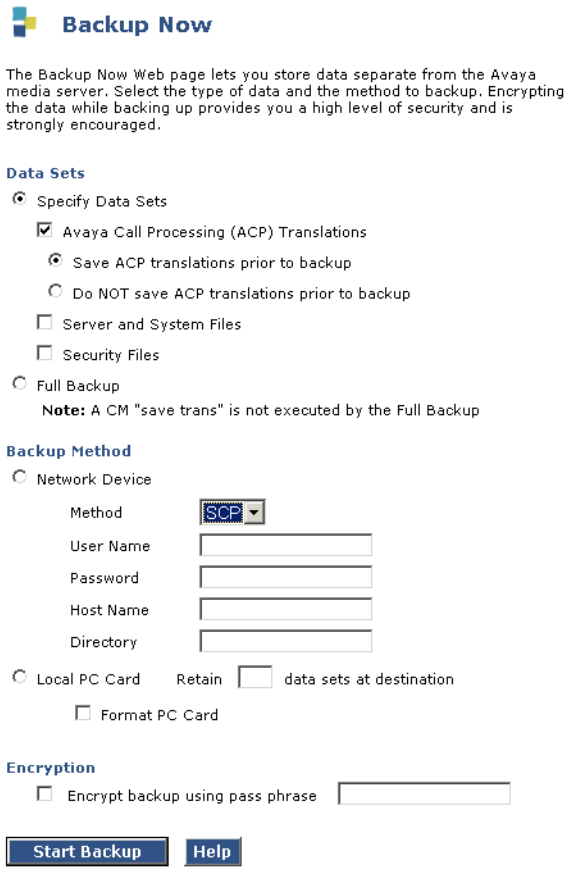
1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

2. From the left side select **Data Backup/Restore > Backup Now**.

   The **Backup Now** page (Figure 84: Backup Now page (S8700 and S8500) on page 356) displays.

Figure 84: Backup Now page (S8700 and S8500)



3. In the **Data Sets** section select the data that you want to back up:
   - **Specify Data Sets** lets you choose these data subsets:
     - **Avaya Call Processing (ACP) Translations** contains Communication Manager administration: stations, trunks, network regions, etc.
       - **Save ACP translations prior to backup**: saves translations to the media server's hard drive before saving to the media that you will specify in the **Backup Method** section (Step 4).
       - **S8700 | 8710** Select this option when you are backing up the *active* media server.
       - **Do NOT save ACP translations prior to backup**: saves translations only to the media that you will specify in the **Backup Method** section on this page (Step 4).

       S8700 | 8710: The **Save ACP translations prior to backup** and **Do NOT save ACP translations prior to backup** fields do not appear when you are logged on to the standby server interfaces.
     - **Server and System Files**: installation-specific configuration files (for example, media server names, IP addresses, and routing information)

- **Security Files**: Avaya Authentication file, logon IDs, passwords or Access Security Gateway (ASG) keys, firewall information, and file monitoring databases

- **Full Backup** saves all files listed above.

4. In the **Backup Method** section select one of the following methods:

   - **Network Device** backs up the data and stores it on the specified network device.

     - **Method**

       FTP (File Transfer Protocol) sends backup data to an FTP server. The FTP server must be available and accessible at the time of the backup, and it must have enough space to store the data.
       SCP (Secure Copy) sets up a SCP session between the server and the network storage device for secure backups.

       Both the FTP and SCP options require the following information:

       - **User Name**: the user's account name.
       - **Password**: the user's password.
       - **Host Name**: the DNS name or IP address of the FTP server.
       - **Directory**: If you want to use the default directory on the FTP server (/var/home/ftp) type a forward slash ("/"); otherwise, type the designated directory path in this field.

   - **Local PC Card**: sends backup data to the PCMCIA card that comes with the media server. This option requires the following information:

     - **Retain __ data sets at destination**: indicate the number of data sets that you want.
     - **Format PC Card**: PCMCIA cards must be formatted before information can be stored. Format the card if it has never been used before or if you want to erase all of the information on the card.

   - **Encryption**: backup data is encrypted through a 15- to 256-character pass phrase (any characters except the following: single quote, backslash, single backquote, quote, and percent).

     SECURITY ALERT:
     Avaya strongly recommends encrypting backup data. Create a pass phrase consisting of letters, numbers, spaces, and special characters for added protection. *You must remember the pass phrase to restore the encrypted data*.

5. Click **Start Backup** to begin the backup process.

   The Backup Now page displays a progress message indicating that the backup is underway.

6. **S8700 | 8710**: Log into and backup the *standby* server by repeating this entire procedure.

Note:

The **Save ACP translations prior to backup** and **Do NOT save ACP translations prior to backup** fields do not appear on standby server interfaces.

S8300 backup procedures

Backing up the Avaya S8300 Media Server involves two major steps:

- Shutting down AUDIX
- Backing up data files

Shutting down AUDIX

Note:

If you are not using IA770 (AUDIX), skip to Backing up data files on page 359.

This procedure gathers IA770 data and shuts down AUDIX:

1. To test IA770 after the backup:
   a. Write down the number of a test voice mailbox, or create one if none exists.
   b. Write down the number of the IA770 hunt group.
2. Leave a message on the test mailbox that will be retrieved after the backup. If you are unsure about how to complete this activity, consult your AUDIX documentation.
3. In the lower-left corner of your laptop/PC, click **Start > Run** to open the Run dialog box.
4. Depending on your connection:
   - If you are directly-connected to the Services port, type **`telnet 192.11.13.6`** and press **Enter**.
   - If you are connected to the network, type **`telnet IPaddress`** and press **Enter**.
5. Log in to the server.
6. Type **`stop -s Audix`** and press **Enter** to shut down AUDIX.

   The shutdown will take a few minutes.

7. Type **watch /VM/bin/ss** and press **Enter** to monitor the shutdown.

   When the shutdown is complete, you will see only the voicemail and audit processes. For example:

   voicemail:(10)

   audit http:(9)

8. Press **Ctrl**+**C** to break out of the **watch** command.
9. Type **/vs/bin/util/vs_status** and press **Enter** to verify that AUDIX is shut down.

   When AUDIX is shut down, you will see “voice system is down.”

Backing up data files

CAUTION:

If the current release of Communication Manager is 1.1.x, you must back up Communication Manager translations (and AUDIX data if IA770 is installed) using this procedure. For Releases 1.2 and later, this backup is optional but recommended.

Tip:

This backup procedure has an FTP option that requires the following information:

- An FTP address
- A directory path
- A user ID and password to access an FTP server on the network

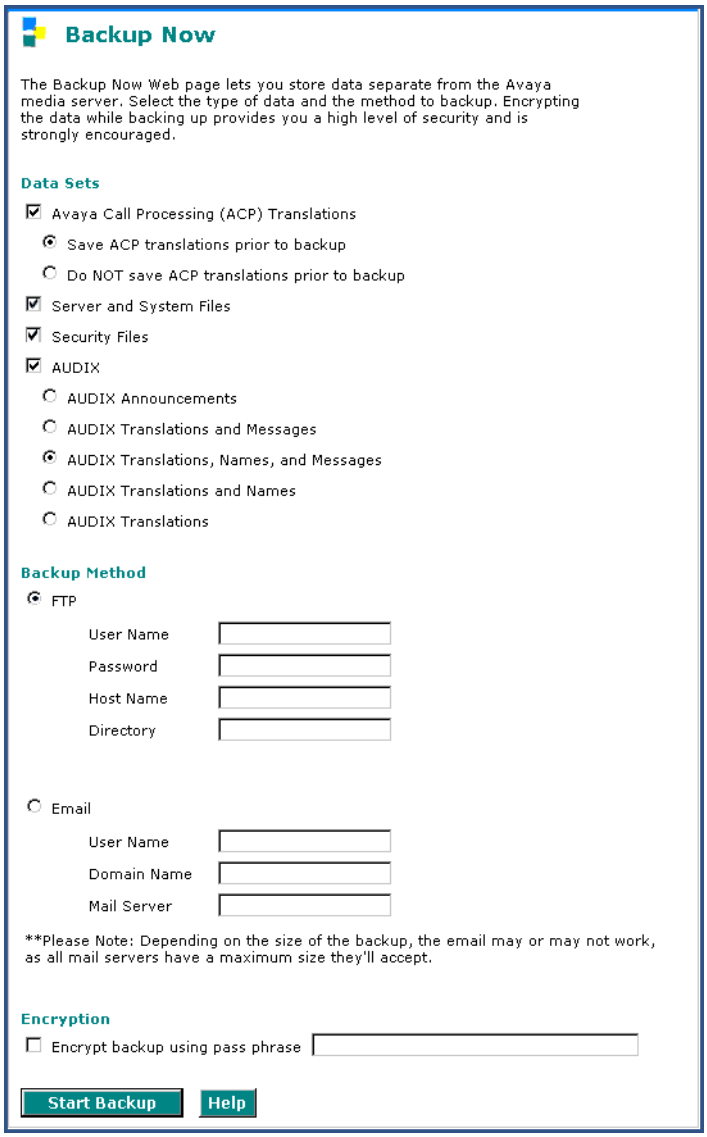
This procedure backs up data files for the Avaya S8300 media server using the Maintenance Web interface:

1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The Integrated Management: Maintenance Web Pages displays.

2. From the left side select **Data Backup/Restore > Backup Now**.

   The **Backup Now** page displays.



3. In the **Data Sets** section select the data that you want to back up:

   - **Avaya Call Processing (ACP) Translations** contains Communication Manager administration: stations, trunks, network regions, etc.)
     - **Save ACP translations prior to backup** saves translations to the media server's hard drive before saving to the media that you will specify in the **Backup Method** section (Step 5). Note: do not choose this option if this is a Local Survivable Processor (LSP).
     - **Do NOT save ACP translations prior to backup**: translations are saved only to the media that you will specify in the **Backup Method** section (Step 5).

- **Server and System Files**: installation-specific configuration files (for example, media server names, IP addresses, and routing information)
- **Security Files**: Avaya Authentication file, logon IDs, passwords or Access Security Gateway (ASG) keys, firewall information, and file monitoring databases

4. If the **AUDIX** options are available, select one of the options (AUDIX Translations, Names, and Messages).

   Note:

   AUDIX announcements must be saved in another backup session. See Step 7.

5. In the **Backup Method** section select one of the following methods:

   - **FTP**: sends backup data to an FTP server. The FTP server must be available and accessible at the time of the backup, and it must have enough space to store the data. This option requires the following information:
     - **User Name**: the user's account name.
     - **Password**: the user's password.
     - **Host Name**: the DNS name or IP address of the FTP server.
     - **Directory**: If you want to use the default directory on the FTP server (/var/home/ftp) type a forward slash ("/"); otherwise, type the designated directory path in this field.
   - **Email**: sends backup data as an email attachment. This option requires that the SMTP in/out, FTP in/out, and Domain out (both TCP & UDP) settings in the **Firewall** page of the Maintenance Web Interface. Type the following information in the respective fields:
     - **User Name**: the user's account name, or the characters preceding the "@" symbol.
     - **Domain Name**: the domain name are those characters following the "@" symbol.
     - **Mail Server**: the mail server's name.

   Note:

   Some e-mail servers/accounts have limits on the file attachment sizes. If your backup data file exceeds the limit, the **Email** option for delivering backup data will not work.

   CAUTION:

   If you choose the **Email** option, there is no way to determine whether the backup was successful or not. Additionally, you cannot restore the backup file unless you move it to a media server-accessible location.

   - **Encryption**: backup data is encrypted through a 15- to 256-character pass phrase (any characters except the following: single quote, backslash, single backquote, quote, and percent).

SECURITY ALERT:

Avaya strongly recommends encrypting backup data. Create a pass phrase consisting of letters, numbers, spaces, and special characters for added protection. *You must remember the pass phrase to restore the encrypted data*.

6. Click **Start Backup** to begin the backup process.

   The Backup Now page displays a progress message indicating that the backup is underway.

7. If the AUDIX options are available, repeat Steps 4 and 5 for AUDIX Announcements.

CAUTION:

If this is a Release 1.x system, you cannot restore AUDIX announcements to a Release 2.0 system, but you should back up these announcements in case it is necessary to revert to the Release 1.x system software.

Backup History

This utility shows the most recent backups for this server.

1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

2. From the left side select **Data Backup/Restore > Backup History**.

   The **Backup History** page () displays.

Figure 85: Backup History page

3. The page lists up to 15 of the most recent backups in reverse chronological order. For example, the first listing is:

   1 sv-gertrude1.111331-20040723.5649

   Interpret the information as follows:

   - **1** is the first backup listed.
   - **sv-gertrude1** is the name of the media server.
   - **111331** is the time of the backup (11 hours, 13 minutes, 31 seconds or 11:13:31 AM).
   - **20040723** is the date of the backup (July 23, 2004).
   - **5649** is the process ID (PID), a unique identifier of this backup.

Schedule Backup

The Schedule Backup page allows you to create (add) a new backup schedule or change or delete a previously-submitted backup for the server. This topic is divided into two tasks:

- Adding or changing a scheduled backup
- Removing a scheduled backup

Adding or changing a scheduled backup

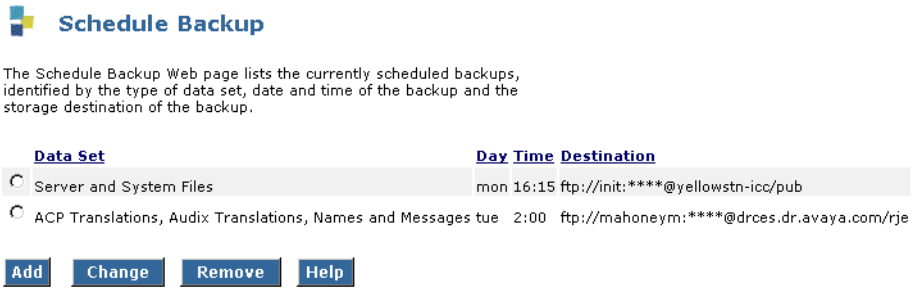
1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

2. From the left side select **Data Backup/Restore > Schedule Backup**.

   The **Schedule Backup** page displays (Figure 86: Schedule Backup page on page 363) any previously-scheduled backups by type.

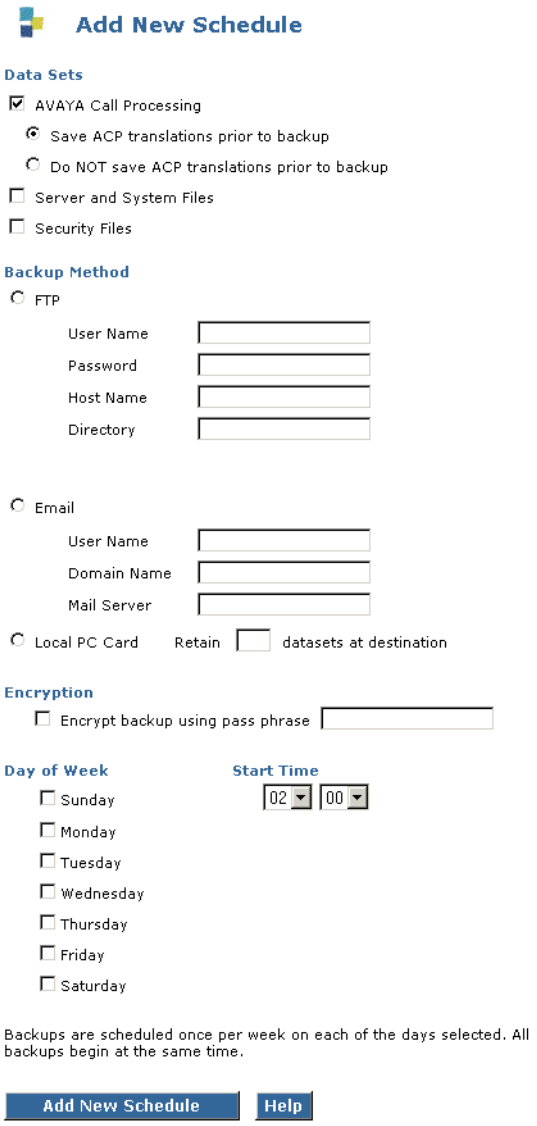
Figure 86: Schedule Backup page



3. Choose to
   - Add a new backup to the schedule by clicking on the **Add** button.
   - Change a previously-scheduled backup by clicking the radio button to the left of the backup listed and clicking on the **Change** button.

   The **Add New Schedule** (Figure 87: Add New Schedule form on page 364) or **Change Current Schedule** page displays, respectively. These forms are the same.

Figure 87: Add New Schedule form



4. In the **Data Sets** section select the data that you want to back up:
   - **Avaya Call Processing (ACP) Translations** contains Communication Manager administration: stations, trunks, network regions, etc.
     - **Save ACP translations prior to backup** saves translations to the media server's hard drive before saving to the media that you will specify in the **Backup Method** section (Step 4).

       S8700 | 8710 Select this option when you are backing up the *active* media server.
     - **Do NOT save ACP translations prior to backup** saves translations only to the media that you will specify in the **Backup Method** section on this page (Step 4).

       S8700 | 8710: The **Save ACP translations prior to backup** and **Do NOT save ACP translations prior to backup** fields do not appear when you are logged on to the standby server interfaces.
   - **Server and System Files**: installation-specific configuration files (for example, media server names, IP addresses, and routing information)
   - **Security Files**: Avaya Authentication file, logon IDs, passwords or Access Security Gateway (ASG) keys, firewall information, and file monitoring databases
5. In the **Backup Method** section select one of the following methods:
   - **FTP**: sends backup data to an FTP server. The FTP server must be available and accessible at the time of the backup, and it must have enough space to store the data. This option requires the following information:
     - **User Name**: the user's account name.
     - **Password**: the user's password.
     - **Host Name**: the DNS name or IP address of the FTP server.
     - **Directory**: If you want to use the default directory on the FTP server (/var/home/ftp) type a forward slash ("/"); otherwise, type the designated directory path in this field.
   - **Email**: sends backup data as an email attachment. This option requires that the SMTP in/out, FTP in/out, and Domain out (both TCP & UDP) settings in the **Firewall** page of the Maintenance Web Interface. Type the following information in the respective fields:
     - **User Name**: the user's account name, or the characters preceding the "@" symbol.
     - **Domain Name**: the domain name are those characters following the "@" symbol.
     - **Mail Server**: the mail server's name.

   Note:

   Some e-mail servers/accounts have limits on the file attachment sizes. If your backup data file exceeds the limit, the **Email** option for delivering backup data will not work.

CAUTION:

If you choose the **Email** option, there is no way to determine whether the backup was successful or not. Additionally, you cannot restore the backup file unless you move it to a server-accessible location.

- **Local PC Card**: sends backup data to the PCMCIA card that comes with the media server. This option requires the following information:
  - **Retain __ data sets at destination**: indicate the number of data sets.
- **Encryption**: backup data is encrypted through a 15- to 256-character pass phrase (any characters except the following: single quote, backslash, single backquote, quote, and percent).

SECURITY ALERT:

Avaya strongly recommends encrypting backup data. Create a pass phrase consisting of letters, numbers, spaces, and special characters for added protection. *You must remember the pass phrase to restore the encrypted data*.

6. Select the **Day of the Week** from the list (once per day, any/all days of the week).
7. Select the **Start Time** from the drop-down boxes. Each day all backups begin at this same time. Avaya suggests avoiding scheduling backups either during peak calling hours or while making administration changes (for example, adds or changes).
8. Click on either the **Add New Schedule** or the **Change Schedule** button.

   The system verifies the request.

Removing a scheduled backup

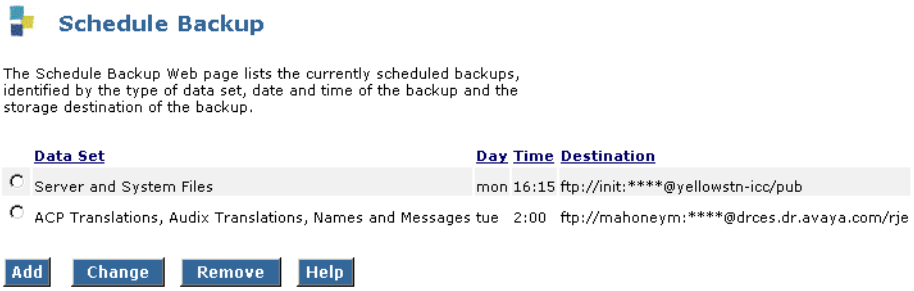
To remove a scheduled backup from the list:

1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.
2. From the left side select **Data Backup/Restore > Schedule Backup**.

   The **Schedule Backup** page (Figure 88) displays any previously-scheduled backups by type.

Figure 88: Schedule Backup page



3. Click the radio button to the left of the scheduled backup that you want to remove.
4. Click on the **Remove** button.

   The system verifies the request.

Backup Logs

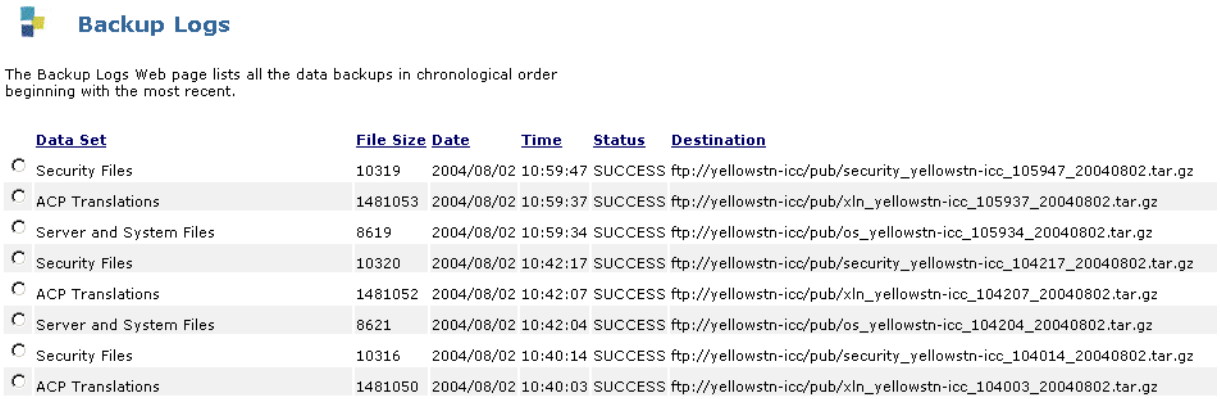
This utility shows a log of backup images for every backup that has been performed on a media server.

1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.
2. From the left side select **Data Backup/Restore > Backup Logs**.

   The **Backup Logs** page displays (Figure 89).

Figure 89: Backup Logs page



The report contains the following information:

- **Data Set**: the type of data:
  - Security Files: contain the Avaya Authentication file, logon IDs, passwords or Access Security Gateway (ASG) keys, firewall information, and file monitoring databases.
  - ACP Translations: contain Communication Manager administration such as stations, trunks, network regions, etc.
  - Server and System Files: contain installation-specific configuration files such as media server names, IP addresses, and routing information.
- **File Size**: physical size of the data set.
- **Date**: year, month, and day of the backup.
- **Time**: hour, minute, and second of the backup.
- **Status**: whether the backup was successful or not.
- **Destination**: indicates how the data was recorded (for example, FTP, email, or local PC card) and the destination address or path.

3. Scan the log until you see a backup image that you want to preview or restore.
4. Select the backup by clicking on the radio button to the left of the log entry.
5. Select one of these buttons:
   - **Preview**: displays a brief description of the data. Use this button if you are not sure that you have selected the correct backup image (see Preview Data).
   - **Restore**: displays detailed information about the backup image.

Note:

If you chose email delivery of your backup data, or if you backed up through FTP but the FTP server does not allow reading, you must first copy (FTP or download) your backup file to the media server before you can restore it.

Preview Data

The **Preview Data** page lists the file destination type, the file path, and name of the backup that you selected in Step 4 above. Depending on the type of backup file, you must supply some required information to preview the information about the file.

Figure 90: Preview Data page

1. If the backup that you selected shows FTP as the destination, then you must supply the same information for the FTP server and encryption that you used at the time of the backup:
   - User Name
   - Password
   - Pass Phrase
2. Press the **Preview** button to see a brief description of the data associated with the backup.

View/Restore Data

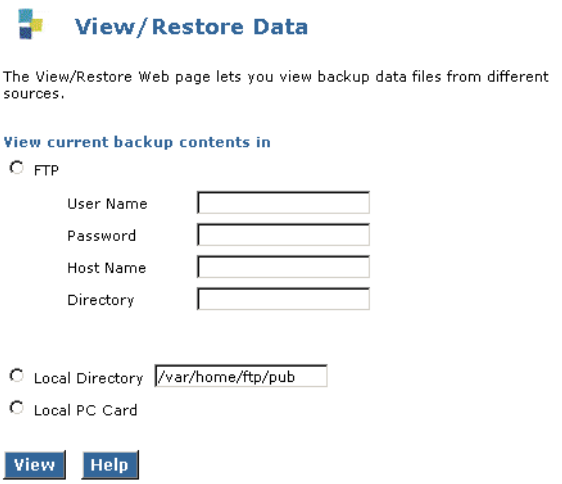
The View/Restore Data utility allows you to browse, preview, and restore backup data files.

1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.
2. From the left side select **Data Backup/Restore > View/Restore Data**.

   The **View/Restore Data** page displays (Figure 91: View/Restore Data page on page 370).

Figure 91: View/Restore Data page



3. Select the source:
   - **FTP**: sends backup data to an FTP server. You must start the FTP server before backing up data. This option requires the following information:
     - **User Name**: the user's account name.
     - **Password**: the user's password.
     - **Host Name**: the DNS name or IP address of the FTP server
     - **Directory**: If you want to use the default directory on the FTP server (/var/home/ftp) type a forward slash ("/"); otherwise, type the designated directory path in this field.
   - **Local Directory**: type the directory path, for example **/var/home/ftp/pub**.
   - **Local PC Card**: displays the contents of the server's PCMCIA card.

   The **View/Restore Data Results** page displays three types of backup files:
   - Avaya Call Processing (ACP) Translations display as:

     /xln_servername_time_date.tar.gz
   - Server and System Files display as:

     /os_servername_time_date.tar.gz
   - Security Files display as:

     /security_servername_time_date.tar.gz
4. Select the file you want to either preview or restore by clicking the radio button to the left of the file.
5. Click on the **View** button.

Restore History

The Restore History utility displays the 15 most recent restores.

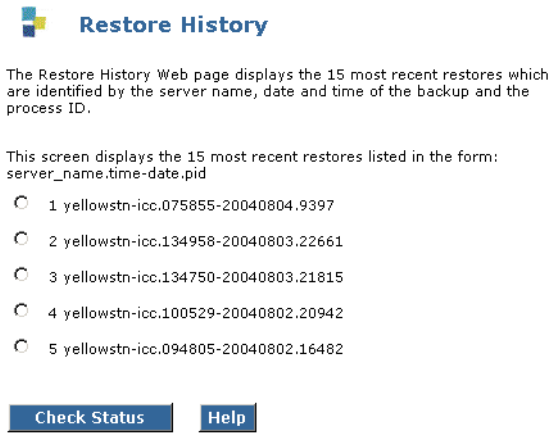
1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

2. From the left side select **Data Backup/Restore > Restore History**.

   The **Restore History** page displays (Figure 92).

Figure 92: Restore History page



3. The page lists up to 15 of the most recent backups, for example:

   1 yellowstn-icc.075855-20040804.9397

   Interpret the information as follows:

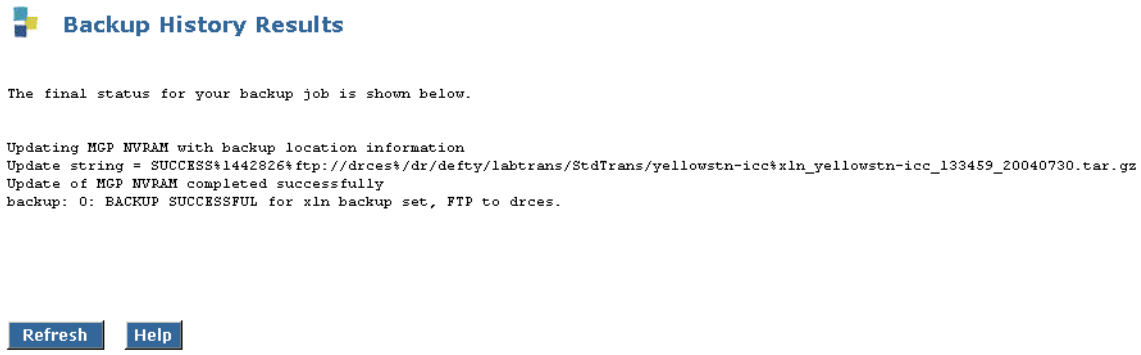
   - **1** is the first backup listed.
   - **yellowstn-icc** is the name of the media server.
   - **075855** is the time of the backup (7 hours, 58 minutes, 55 seconds or 7:58:55 AM).
   - **20040804** is the date of the backup (April 8, 2004).
   - **9397** is the process ID (PID), a unique identifier of this backup.

4. If you want to check the status of a backup, select the file by clicking the radio button to the left of the file.

5. Press the **Check Status** button.

   The **Backup History Results** page displays.

Figure 93: Backup History Results page



6. The status of the selected backup is displayed. Click on the **Refresh** button to update the list.

Format PC Card

The Format PC Card utility prepares the PCMCIA card that comes with the server for data. A new card only needs to be formatted once.

WARNING:
Clicking on the **Format** button erases any existing data on the card.

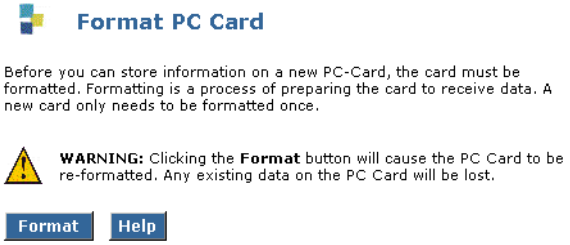
1. After logging into the Integrated Management: Standard Management Solutions (Web interface), in the Maintenance section select **Launch Maintenance Web Interface**.

   The **Integrated Management: Maintenance Web Pages** displays.

2. From the left side select **Data Backup/Restore > Format PC Card**.

   The **Format PC Card** page displays (Figure 94).

Figure 94: Format PC Card page



3. Ensure that the PCMCIA or Compact Flash card is in the proper slot.
4. Click on the **Format** button.

   The system asks whether you want to format the PC card (see Warning above).
5. Click on **Yes** to continue.

Chapter 12: Component replacement

This chapter describes how to replace components in the system. It includes the following topics:

- Variable-speed fans on page 375
- Reseating and replacing circuit packs on page 378
- CMC1 component maintenance on page 379
  - Replacing fans and air filters (CMC1) on page 379
- S8300 component maintenance on page 380
- S8500 component maintenance on page 381
- S8700 component maintenance on page 381
- G650 component maintenance on page 382
  - G650 fan removal/replacement on page 382
- Replacing a BIU or rectifier on page 383

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.

To replace the fan power filter:

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.

Special procedures

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.

CAUTION:
Table 66 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) If the IPSI has a static IP address, refer to Re-using an IPSI circuit pack.
TN768 TN780 TN2182B	Tone-Clock Tone-Clock 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

CMC1 component maintenance

Replacing fans and air filters (CMC1)

Air filters on the CMC1 should be inspected annually. (See Table 67.)

Table 67: Inspecting air filters

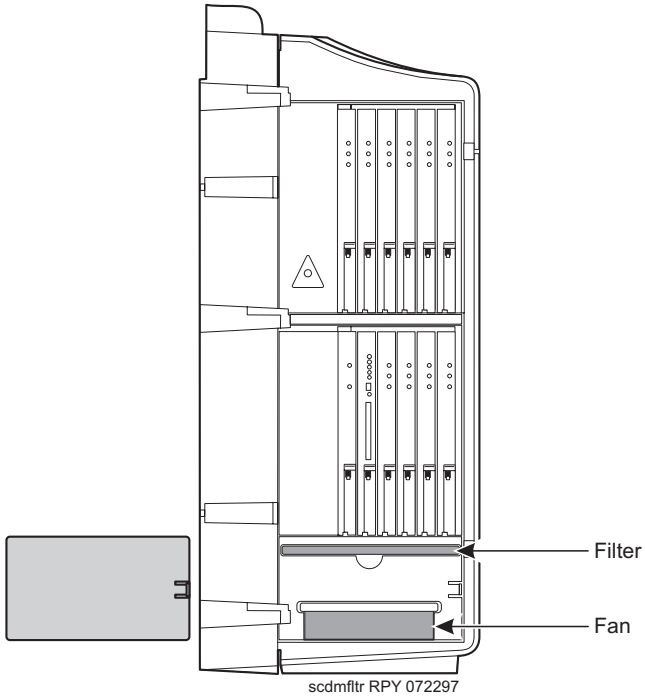
If	Then
Filter is dirty or clogged	Tap filter on the ground.
Tapping does not dislodge dirt or clog	Wash with warm water and mild detergent, or clean with a vacuum cleaner (if one is available).
No facility exists for washing or vacuuming	Replace air filter. Refer to Figure 95: Fan/filter removal on page 380 for more information on air filters and fans.

Fan filter removal/replacement

To replace the fan filter:

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 95: Fan/filter removal on page 380).
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 95: Fan/filter removal



S8300 component maintenance

See *Job Aids for Field Replacements (FRUs) for the Avaya S8300 Media Server with the G700 Media Gateway, 03-300538* for these procedures:

- Job Aid: Replacing the S8300 Media Server or its Hard Drive*
- Job Aid: Replacing the G700 Media Gateway
- Job Aid: Replacing Media, Expansion, or Octaplane Modules

S8400 component maintenance

Job Aids for Field Replacements (FRUs) for the Avaya S8400 Media Server, 03-300623 contains these procedures:

- Job Aid: Replacing the Avaya S8400 Media Server
- Replacing the hard drive on the Avaya S8400 Media Server
- Replacing the server interface circuit pack on the Avaya S8400 Media Server
- Replacing the solid state drive on the Avaya S8400 Media Server

S8500 component maintenance

Job Aids for Field Replacements (FRUs) for the Avaya S8500 Media Server, 03-300529 contains these procedures:

- Job Aid: Replacing the RSA
- Job Aid: Replacing the Dual Network Interface
- Job Aid: Replacing the S8500 Hard Drive
- Job Aid: Replacing the S8500 Media Server
- Job Aid: Replacing the SAMP
- Job Aid: Replacing the SAMP power supply
- Job Aid: Replacing the USB modem
- Job Aid: Replacing the Compact Flash reader and card
- Job Aid: Replacing the IP Server Interface

S8700 component maintenance

See *Job Aids for Field Replacements (FRUs) for the Avaya S8700 Series Media Servers, 03-300530* for these procedures:

- Job Aid: Replacing the S8700 Media Server Pre-R2.0)
- Job Aid: Replacing the Hard Drive in the S8700 Media Server (Pre-R.2.0)*
- Job Aid: Replacing the Hard Drive in the S8700 Media Server, Release 2.0 and later*

- Job Aid: Replacing the S8700 Media Server - Release 2.0 and later
- Job Aid: Replacing the Hard Drive in the S8700 Media Server (R2.2 and later)*
- Job Aid: Replacing the USB modem
- Job Aid: Replacing the IP Server Interface
- Job Aid: Replacing the SanDisk flash memory
- Job Aid: Replacing the Avaya S8710 Media Server
- Job Aid: Replacing the Hard Drive in an Avaya S8710 Media Server
- Job Aid: Replacing the Avaya S8720 Media Server
- Job Aid: Replacing the Hard Drive in an Avaya S8720 Media Server
- Job Aid: Replacing the DAL1 in an Avaya S8720 Media Server
- Job Aid: Replacing the quad NIC in an Avaya S8720 Media Server

G650 component maintenance

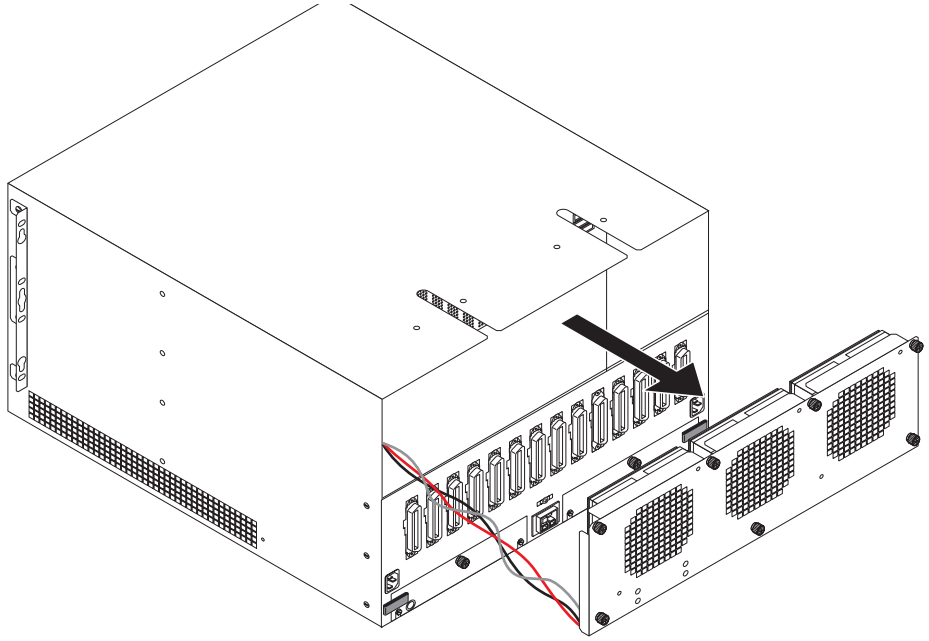
G650 fan removal/replacement

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.

To replace a G650 fan:

1. Place the new fan assembly close to the G650.
2. Loosen the thumb screws on the fan assembly, and pull it straight out as shown in Figure 96: Removing the G650 fan assembly on page 383.

Figure 96: Removing the G650 fan assembly



3. Disconnect the fan cable.
4. Connect the new cable and position the new fan assembly.
5. 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.

Chapter 13: Packet and serial bus maintenance

The topics covered in this chapter include:

- Isolating and repairing packet-bus faults on page 385
- G650 Serial Bus fault detection and isolation on page 415

Isolating and repairing packet-bus faults

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 386 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 386 discusses the tools that are needed to isolate and correct packet-bus faults.
- What is the packet bus? on page 387 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 389 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 391 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 394 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 402 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 407 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 397.
- A backplane pin-replacement kit may be required (see Correcting packet-bus faults on page 407). 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 389.

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 (ISDN-BRI Line Circuit Pack)
  - BRI-PORT (ISDN-BRI Port)
  - BRI-SET, 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 on page 392
- Packet Bus maintenance software on page 393
- General fault correction procedures on page 393

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 393).

- **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)
- 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 might 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. **Note:** 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 *port01***, **busyout port *port02***, and **busyout port *port03***. 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 395), 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 402.
- 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 Material ID 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 97.

Figure 97: 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” displays, 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 98: Stand-alone mode display on page 399 shows the state of the packet bus leads.

Figure 98: Stand-alone mode display

```
L L L L L L L L L 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 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 99: Packet bus leads on the backplane (front view) on page 400 shows the location of the packet bus leads for a given slot as seen from the front and back of the carrier.

Figure 99: Packet bus leads on the backplane (front view)

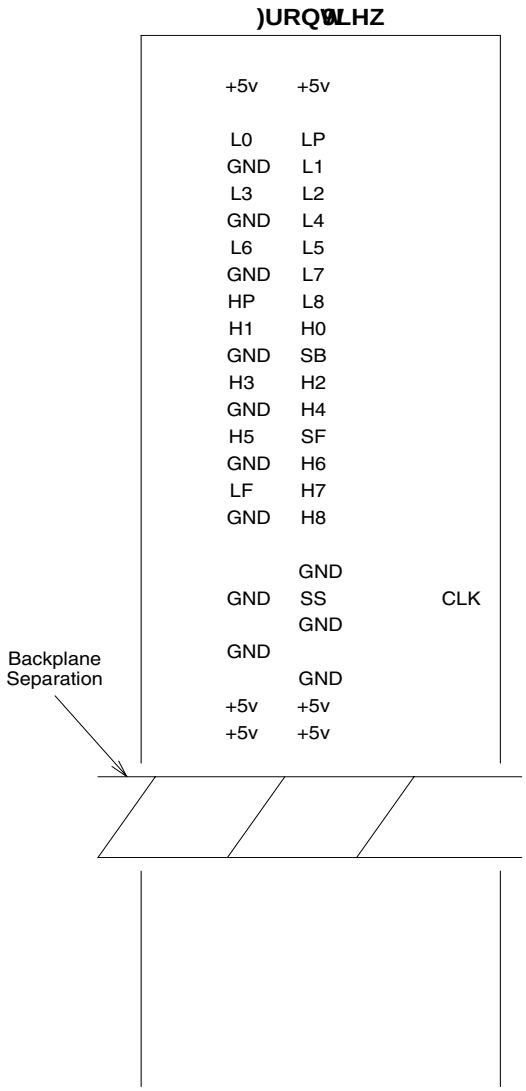
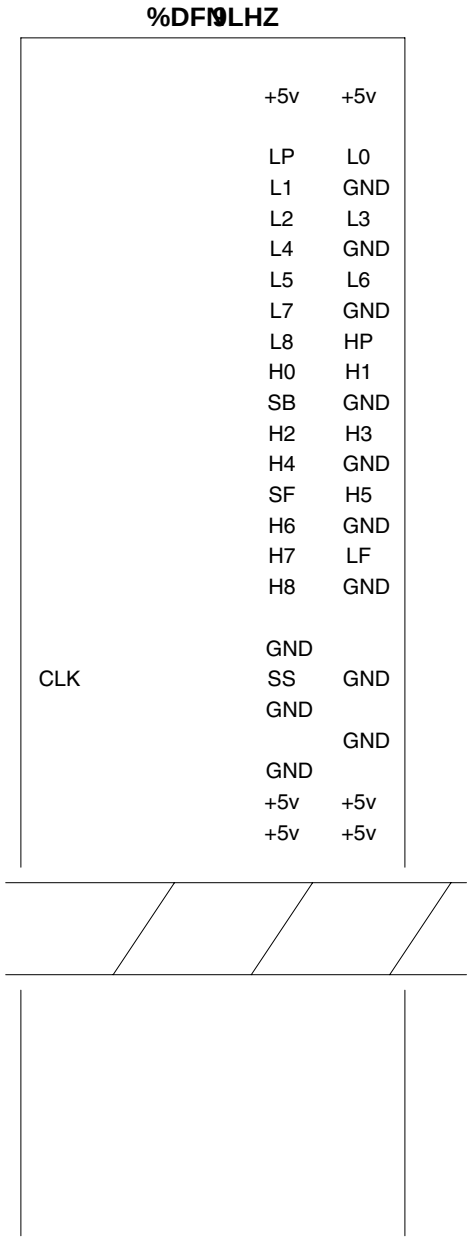


Figure 100: Packet bus leads on the backplane (rear view) on page 401 shows the location of the packet bus leads for a given slot as seen from the front and back of the carrier.

Figure 100: 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 *location***.
5. Replace the Maintenance/Test circuit pack with the new circuit pack.
6. Release the Maintenance/Test circuit pack with **release board *location***.
7. Enter the **test pkt *P*** and **status port-network *P*** commands.
8. If the data match the previously recorded data, a packet bus problem exists, and the original TN771D Maintenance/Test circuit pack is not defective. Re-insert 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

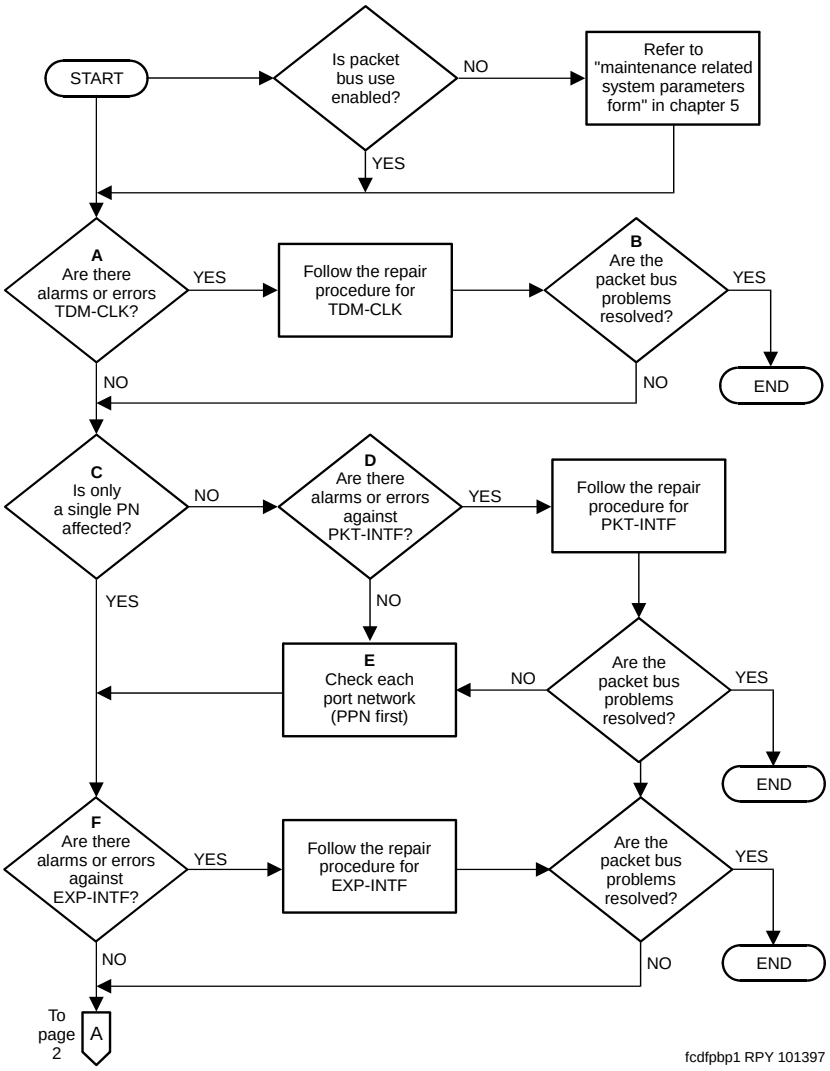
Figure 101: Troubleshooting packet-bus problems (1 of 2) on page 404 and Figure 102: Troubleshooting packet-bus problems (2 of 2) on page 405 show the steps to be taken for isolating and resolving a packet-bus problem. The order of examining maintenance objects (MOs) can be determined by assessing how 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**

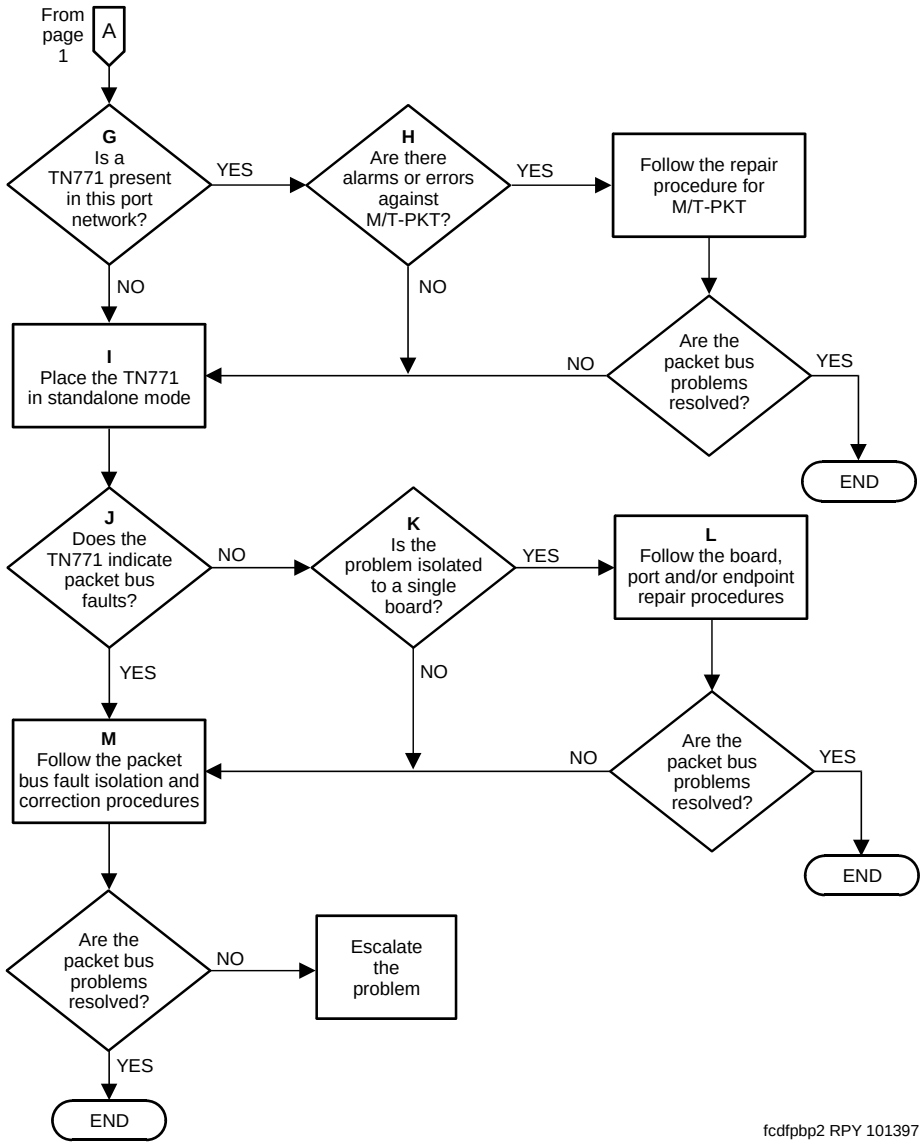
Figure 101: Troubleshooting packet-bus problems (1 of 2)



Note:

Bold-face letters in the flowchart are explained in Flowchart notes on page 406.

Figure 102: Troubleshooting packet-bus problems (2 of 2)



Note:

Bold-face letters in the flowchart are explained in Flowchart notes on page 406.

Flowchart notes

The following paragraphs refer by letter to corresponding entries in Figure 101: Troubleshooting packet-bus problems (1 of 2) on page 404 and Figure 102: Troubleshooting packet-bus problems (2 of 2) on page 405. 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.

1. 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.
2. 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?
3. 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.
4. 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.
5. 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.
6. If a TN771D is absent, one must be installed to accommodate the stand-alone mode. See the previous section on stand-alone mode.
7. 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.
8. 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.

9. 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.
10. If the non-functional endpoints are isolated to a single circuit pack, then that circuit pack is probably the cause of the problem.
11. Investigate errors and alarms in the following order:
    - Circuit-pack level
    - Ports
    - Endpoints
12. Follow the Troubleshooting procedures on page 409. 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 *P*** 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 *P*** 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 *location***. If any problems are suspected, see Special precaution concerning the TN771D on page 402.

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 P`**, 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 | 8710 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 409.

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 414. 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 414, 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 68: Packet circuit packs on page 410 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 68: Packet circuit packs

Circuit Pack Name	Code	Associated maintenance objects
ISDN-BRI	TN556	BRI-BD BRI-PORT ABRI-PORT BRI-SET BRI-DAT ASAI-ADJ
Maintenance/Test	TN771D	M/T-BD, M/T-PKT
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: removing and reinserting a PN's control circuit packs on page 412 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 410, 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 68: Packet circuit packs on page 410 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.

If the packet-bus fault is still present:

3. 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.
   - If the backplane pins are bent:
     - Power down the carrier.
     - Straighten or replace the pins.
     - Reinsert the circuit pack.
     - Restore power.
     - Repeat Step 2 for the same circuit pack.
   - If the backplane pins are not bent:
     - Reinsert the circuit pack(s)
     - Repeat this procedure for the next set of circuit packs.

4. If the packet-bus fault is not present:
   - Reinsert circuit packs one at a time and repeat the following substeps until every circuit pack has been reinserted.
   - Determine whether the packet-bus fault has returned.
   - If the packet-bus fault has returned, the reinserted circuit pack is defective. Replace the circuit pack and then continue.
   - 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 412 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 | 8710 only

Systems with nonduplicated SPEs

To repair packet bus faults in 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.
7. If the problem is still present, continue:
   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: isolating failures.

High- and critical-reliability systems

In high-and critical-reliability configurations:

1. To remove a PN's IPSI circuit pack, use **`set ipserver-interface`** ***`location`*** 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`** ***`P`***.)

   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 414.

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 103: Carrier rewiring example—rear view of MCC1 on page 414). 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.

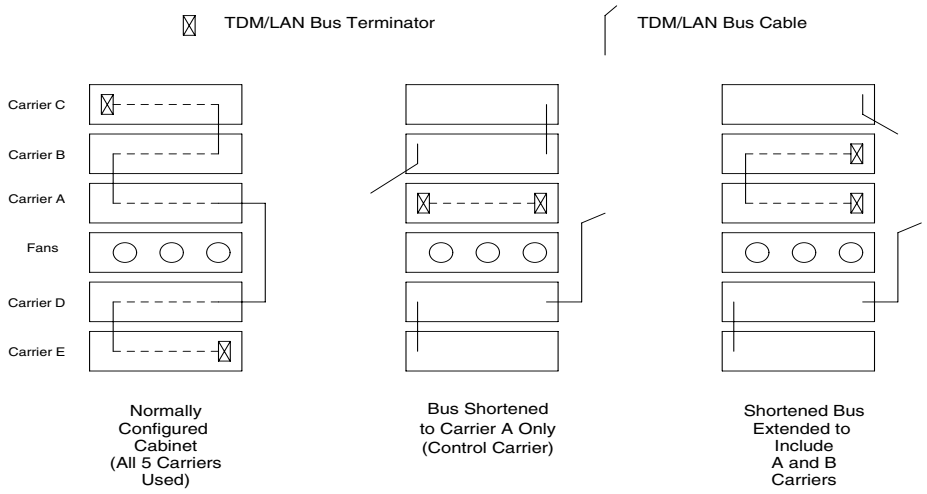
DANGER:

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 103: Carrier rewiring example—rear view of MCC1



Procedure 4 consists of two parts. Part 1 on page 415 attempts to clear the packet-bus fault by replacing every bus cable and terminator within a PN. Part 2 on page 415 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 415.

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.

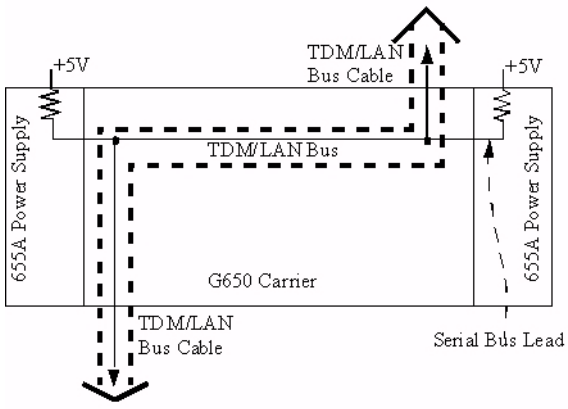
G650 Serial Bus fault detection and isolation

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 104: 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

To replace all bus cabling and terminators:

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

To isolate the fault to a particular carrier:

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.

Chapter 14: Additional maintenance procedures

This chapter describes updates, tests and preventive measures not covered elsewhere in this book. It includes the following topics:

- SBS maintenance on page 421
- Re-using an IPSI circuit pack on page 427
- Updating software, firmware, and BIOS on page 431
- DS1 CPE loopback jack (T1 only) on page 432
- Facility test calls on page 445
- Call Admission Control-Bandwidth Limitation on page 456
- TN760E tie trunk option settings on page 470
- Removing and restoring power on page 474
- Automatic Transmission Measurement System on page 481
- Setting G700 synchronization on page 493
- IP Telephones on page 498

SBS maintenance

No Media Processor issues

The Separation of Bearer and Signal (SBS) functionality means that SBS trunks do not carry the bearer (audio) portion of a SBS call, and thus do not require Media Processor (VoIP Engine) resources. SBS trunks have different maintenance behavior than "regular" H.323 IP trunk groups, for example, they can be brought into service as soon as the associated signaling group is in service.

Each SBS signaling trunk group requires an assigned signaling group that is administered on the Signaling Group form.

Communication Manager administrators can define system-wide acceptable limits of round-trip delay and packet loss on the **System Parameters Maintenance** form, **IP** page (**`change signaling-group`**). If the **Bypass if IP thresholds exceeded?** field for H.323 signaling groups is set to "yes" and the IP thresholds are exceeded, the signaling group and its associated IP trunks are placed in maintenance bypass mode. This means that:

- Idle trunks are taken out of service, making them unavailable for new outgoing calls.
- Active trunks are taken out of service *after* the existing call drops.

Since IP network congestion can be one source of delay in establishing SBS calls, Communication Manager administrators could consider utilizing this "bypass" mechanism to ensure acceptable SBS feature operation. However, the system-wide packet delay/loss parameters are typically administered to ensure proper voice quality and might be more restrictive than necessary for signaling-only calls. In other words, **Bypass could cause SBS trunks to be taken out of service unnecessarily** when delays are disruptive to voice quality, but not severe enough to have a noticeable impact on the overall SBS call setup delay. Avaya recommends that you carefully consider the system-wide packet loss and delay settings before implementing Bypass on SBS signaling groups.

Also, the periodic background tests that drive the Bypass capability require Media Processor resources, and if there are none, which is possible because SBS trunks do not require media processor resources, the Bypass test does not execute and no Bypass occurs.

Signaling group maintenance

H.323 signaling group maintenance is also performed on SBS signaling groups. Signaling group failures are detected when a TCP signaling connection cannot be established to the far-end for originating a new call, and maintenance is notified to run the appropriate signaling group tests. In normal circumstances once maintenance drives the faulty signaling group out of service, subsequent calls cannot use the associated signaling trunk group. However, maintenance might not place the faulty SBS signaling group out of service immediately. During this variable time interval, all outgoing call attempts using this signaling group, including the first call that detected the fault, are internally rejected with a Look Ahead Routing (LAR) triggering Cause Value. If LAR is enabled on the appropriate route-pattern preference for this SBS trunk group, alternate preferences are attempted until the trunk group is finally taken out of service.

SBS trunk service states

SBS trunk group members achieve "in service" status without requiring that any associated Media Processor circuit packs be in service. All that is required for an SBS trunk group member to be "usable" for a call is that the associated signaling group reach an "in service" state.

When a SBS signaling group goes out of service for any reason, the associated SBS trunk group members associated with that signaling group are taken out of service to avert failed call attempts. Reasons that a signaling group might be taken out of service include busy out of the signaling group, or CLAN board removal or failure.

The status of Media Processor resources, if present, does not have any effect on SBS trunk group member service states.

Trunk member status

The **`status trunk`** ***`trunk group/member`*** command, when executed against a SBS trunk group member, shows the associated bearer trunk port in the **Associated SBS port** field.

Conversely, if the **`status trunk`** ***`trunk group/member`*** command is executed against a bearer trunk group member involved in a SBS call, the associated SBS trunk group member is displayed.

SBS extension status

When the **`status station`** command is executed for an SBS Extension the results are the same as any Administered Without Hardware extension.

Note:

SBS Extensions are active only for short periods of time during call setup.

Finding the parties Involved in an SBS Call

At an SBS Originating Node the parties involved in an SBS call can be determined via status commands, as shown in Parties Involved in an SBS Call on page 424.

At an SBS Terminating Node the parties involved in an SBS call can be determined in a similar fashion to that described for the SBS Originating Node by replacing the "originating" station/trunk with the "terminating" station/trunk, and replacing the "outgoing" bearer trunk with the "incoming" bearer trunk.

At an SBS Tandem Node executing "status trunk" on an SBS trunk member will show that the trunk is "in-service/active." However, the **Connected Ports** and **SBS Associated Port** fields will be blank. *This should not be misinterpreted as a hung trunk.* The associated bearer call will most likely route entirely through the PSTN. Even if the associated SBS bearer call routes through the SBS Tandem Node, that node will have no way of associating the SBS signaling and SBS bearer calls. Association of the signaling and bearer calls can only be accomplished at the SBS Originating and SBS Terminating Nodes.

Table 69: Parties Involved in an SBS Call

SBS Originating Node		
Command	**Shows Connected Ports**	**Shows SBS Associated Port**
Status on originating station or incoming non-SBS trunk. **status station** *n* or **status trunk-group**/member	Outgoing bearer trunk port	n/a
Status on outgoing bearer trunk group *status trunk-group*	Originating station or incoming non-SBS trunk	n/a
Status on outgoing bearer trunk group member status trunk-group/member	Originating station or incoming non-SBS trunk	Outgoing SBS trunk port
Status on outgoing SBS trunk group *status trunk-group*	Originating station or incoming non-SBS trunk	n/a
Status on outgoing SBS trunk group member *status trunk-group/member*	Originating station or incoming non-SBS trunk	Outgoing bearer trunk port

Errors and denial events

Software errors and denial events are logged for the error conditions and cause values listed in Error Conditions on page 425 along with the tone treatment provided to the originating party, whether or not Look Ahead Routing (LAR) is attempted, and the type of event.

Table 70: Error Conditions *1 of 2*

Error Condition	Cause Value	LAR or non-LAR	Tone Treatment	Software Error or Denial Event
SBS Orig. Node gets CALL PROC w/o Null Caps, or gets ALERT, PROG, or CONN before 2 INFO msgs, or gets INFO w/bad contents	95 (invalid msg)	Non-LAR	Intercept	Denial event
SBS Term. Node gets bearer call to allocated SBS Extension, but wrong call	21 (call rejected)	Non-LAR	Reorder	Error
SBS Term. Node has SBS Extensions administered but none available	47 (resource unavailable, unspecified)	LAR	Reorder	Denial event
SBS Term. Node has no SBS Extensions administered	69 (requested facility not implemented)	Non-LAR	Intercept	Denial event
SBS Term. Node allocates SBS Extension but can't map it to National Complete Number	79 (service/ option not implemented, unspecified	Non-LAR	Intercept	Denial event
SBS Term. Node gets incoming trunk call to non-allocated SBS ext.	21 (call rejected)	Non-LAR	Reorder	Error
SBS Term. Node gets local endpoint call to SBS Extension (allocated or not)	N/A	N/A	Intercept	Error
SBS Term. Node gets incoming trunk call to SBS Extension that already has 2 trunk calls	21 (call rejected)	Non-LAR	Reorder	Error
SBS Term. Node gets SETUP w/o Null Caps	95 (invalid msg)	Non-LAR	Intercept	Denial event

1 of 2

Table 70: Error Conditions *2 of 2*

Error Condition	Cause Value	LAR or non-LAR	Tone Treatment	Software Error or Denial Event
Non-SBS trunk gets SETUP or CALL PROC with NULL CAPS	95 (invalid msg)	Non-LAR	Intercept	Denial event
Percentage of SBS Extensions in use (allocated) exceeds 80%	N/A	N/A	N/A	Denial event

2 of 2

System resets

All reset levels act upon SBS trunk calls in the same manner they act on other types of trunk calls. A reset level 2 or higher causes any SBS trunk call to be dropped. The signaling and bearer portions of the SBS trunk call are dropped and all facilities associated with the SBS trunk call re-initialized. All administered SBS extensions are placed in the *available* state (to call processing) after a level 2 or higher reset.

A hot restart or a warm restart (reset level 1) do not affect existing stable SBS calls.

Upgrades

SBS calls are *not* preserved during an upgrade.

Duplication interactions

Scheduled or demand processor/server interchanges have no impact on SBS calls.

Traffic measurement

Traffic measurements for SBS calls and resources use existing measurements.

For SBS signaling and associated bearer trunk groups, use the **`list measurements trk-grp hourly/summary`** command for traffic measurements.

No new measurements are implemented for SBS Extensions. The usage of SBS Extensions is very transient. However, if a SBS Terminating Node is out of SBS Extensions to allocate, an error will be logged. Use the **`display errors`** command for the incoming SBS trunk group to display these errors.

Listing station types

To find assigned SBS extensions:

1. Type **`list stations type sbs`** and press **Enter**.

   The system displays the **Stations** form (Figure 105) that shows the administered SBS extensions.

2. Press **Enter** to save the screen.

Figure 105: Stations screen

```
list station type sbs                                                Page   1

                                  STATIONS

          Port/     Name/                        Room/          Cv1/ COR/     Cable/
Ext       Type      Hunt-to              Move    Data Ext       Cv2  COS      Jack

694101    X         SBS EXTENSION                                    1
          SBS                            no                        1
694102    X         SBS EXTENSION                                    1
          SBS                            no                        1
694103    X         SBS EXTENSION                                    1
          SBS                            no                        1
694105    X         SBS EXTENSION                                    1
          SBS                            no                        1
694106    X         SBS EXTENSION                                    1
          SBS                            no                        1
694107    X         SBS EXTENSION                                    1
          SBS                            no                        1
694108    X         SBS EXTENSION                                    1
          SBS                            no                        1
```

Re-using an IPSI circuit pack

If you are re-using TN2312AP or TN2312BP (IPSI) circuit packs, you might have to change the IPSI addressing parameters. The likely scenarios for doing this are when

- Moving from dynamic to static addressing
- Moving from static to dynamic addressing
- An IPSI is configured with dynamic (DHCP) addressing at a staging area to more easily facilitate firmware upgrades before installation at customer site.

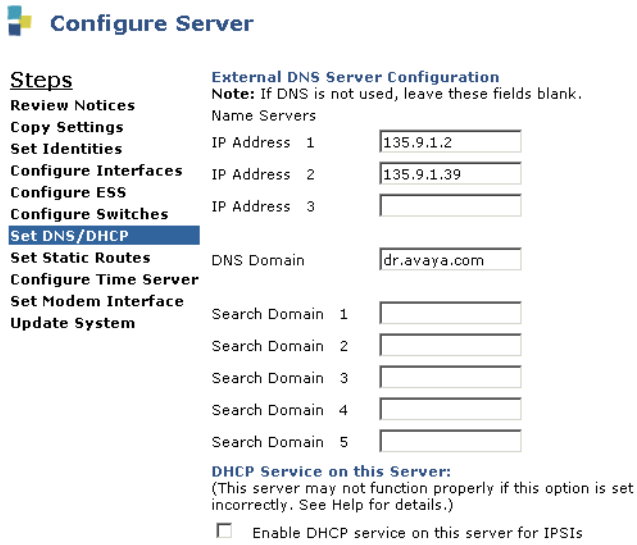
CAUTION:

Failure to erase the existing IP address before re-using the IPSI circuit pack can create serious network problems.

Moving from dynamic to static addressing

To change a TN2312AP/BP IPSI from a DHCP address configuration to a static IP address configuration:

1. At the Maintenance Web Interface select **Server Configuration > Configure Server**.



2. Ensure that the **Enable DHCP service on this server for IPSIs** field is *not* checked.
3. Plug the circuit pack into the appropriate slot in the media gateway or if already plugged in, reseat it (unplug and replug).
4. Wait until the first letter (Switch ID) and the first (cabinet) digit on the LED display stops flashing (approximately 10 seconds), then press the recessed pushbutton on the faceplate to change the *second* digit to **0**.

   The LED display should now read **A00**.
5. Telnet to the IPSI using **`telnet 192.11.13.6`**.
6. At the IPSI prompt, enter **`ipsilogin`** to log in to the IPSI IP Admin Utility.
7. Log in using **craft** and the IPSI password.
8. Type **`set control interface ipaddr netmask`** and press **Enter**.
9. If required, set the gateway IP address (**`set control gateway gateway`**, where gateway is the IP customer-provided IP address for their gateway).

10. Type **quit** to save the changes and exit the session. *Do not reset the IPSI circuit pack at this time.*

    Note:

    If you reset the IPSI, this procedure will not work, and the IP address of the IPSI will display as **0.0.0.0**.

11. Telnet to 192.11.13.6 and login.
12. If a default gateway is used, enter the gateway IP address using **set control gateway *gatewayaddr***.
13. Enter **quit** to save the changes and exit the IPSI session.
14. Telnet to 192.11.13.6 and login.
15. Use **show control interface** to verify the administration.
16. Enter **quit** exit the IPSI session.

If required, set the VLAN and diffserv parameters.

1. Telnet to the IPSI and log in.
2. Type **show qos** to display the current quality of service parameters values.
3. Use the following set commands with their recommended values, if necessary:

   set vlan priority 6

   set diffserv 46

   set vlan tag on

   set port negotiation 1 disable

   set port duplex 1 full

   set port speed 1 100

4. Type **show qos** to display the administered quality of service parameters values.
5. Ensure that your Ethernet switch port settings match the settings above.

Reset the IPSI and exit the IPSI IP Admin Utility.

1. Telnet to 192.11.13.6 and login.
2. Enter **reset**.

   Enter **y** in response to the warning.

3. Disconnect the laptop from the IPSI.
4. Verify that the LED on the IPSI faceplate displays "IP" and a filled-in "V" at the bottom.
5. Repeat these steps for each of the other new IPSIs.

   Note:

   Clear the ARP cache on the laptop before connecting to another IPSI by entering **arp -d 192.11.13.6** at the Windows command prompt.

Verify the IPSI translations

After all of the IPSIs have been administered, verify IPSI translations and connectivity:

1. At the SAT, enter **`list ipserver-interface`** to view the interface information for all of the IPSIs.

   The State of Health - C P E G column should show **0.0.0.0** for each IPSI. If a "1" shows in any position, you must troubleshoot the problem.

   Tip:
   The pattern **0.1.1.0** usually means there is a wrong cabinet type administered or a connectivity problem, such as an improperly terminated cable.

2. On the Maintenance Web Interface under Diagnostics, select **Ping**.

   a. Select **Other server(s), All IPSIs, UPS(s), Ethernet switches**.

   b. For all IPSIs, the **#Mess Sent** (number of messages sent) should equal **#Mess Recv** (number of messages received).

Moving from static to dynamic addressing

To change a TN2312AP/BP IPSI from a static IP address configuration to a DHCP (dynamic) address configuration:

1. Plug the circuit pack into the appropriate slot in the media gateway or if already plugged in, reseat it (unplug and replug).
2. While “IP” flashes on the display, push the recessed button on the IPSI faceplate.

   The display changes to **A00** with the first character (A) flashing.
3. Push the recessed button to program the server ID and cabinet number for DHCP addressing.

Updating software, firmware, and BIOS

Use the information sources listed in Table 71 to update software, firmware, or BIOS on Avaya equipment.

Table 71: Firmware upgrade information sources *1 of 2*

Equipment	Information source
TN circuit packs	• FW-DWNLD (Firmware Download) in *Maintenance Alarms Reference (03-300430)* • Lists of available firmware and a compatibility matrix is located at support.avaya.com, then select **Technical Database > Software & Firmware Downloads > Communication Manager/DEFINITY Servers**.
S8500 Media Server	*Job Aid: Upgrading Firmware on the BIOS—Avaya S8500 Media Server, 03-300411* • Upgrading firmware on the IPSIs • Upgrading firmware on the Avaya Ethernet switch • Upgrading firmware on the maintenance adapter • Upgrading firmware on the BIOS Remote Supervisor Adapter: “Updating RSA or BIOS firmware” in the *The Avaya RSA Users’ Guide, 555-245-702.*
S8700 Series Media Server	*Upgrading, Migrating, and Converting Media Servers and Gateways, 03-300412* • Upgrading firmware on the IPSIs • Upgrading firmware on the Avaya Ethernet switch
	1 of 2

Table 71: Firmware upgrade information sources *2 of 2*

Equipment	Information source
G700 Media Gateway	*Job Aid: Firmware Download Procedure for the G700 Media Gateway, 555-245-758* • Processors - C360 Stack Processor (Layer 2 switching processor) - Media gateway processor (MGP) - Internal VoIP processor • Media Modules - MM710 (T1/E1) - MM711 (Analog) - MM712 (DCP) - MM714 (Analog) - MM717 (DCP) - MM720 (BRI) - MM722 (BRI) - MM760 (VoIP)
4600 Series phones	FW-STDL in *Maintenance Alarms Reference (03-300430)*

2 of 2

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 106: Network Interface at Smart Jack on page 439.
2. If there is an extended demarcation point and the smart jack is not accessible, install the loopback jack as shown in Figure 107: Network Interface at Extended Demarcation Point (Smart Jack inaccessible) on page 440.
3. If there is an extended demarcation point, but the smart jack is accessible, install the loopback jack as shown in Figure 108: Network Interface at Extended Demarcation Point (Smart Jack accessible) on page 441.

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 109: Network Interface at “Dumb” Block on page 442 and Figure 110: Network Interface at “Dumb” Block with repeater line to Fiber MUX on page 443.

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 106: Network Interface at Smart Jack on page 439 through Figure 110: Network Interface at “Dumb” Block with repeater line to Fiber MUX on page 443.
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

To administer the loopback jack:

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.

To test the DS1 span:

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 72: DS1 span troubleshooting on page 435 for troubleshooting information.

Table 72: DS1 span troubleshooting *1 of 2*

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. • If **n** appears, retry the test five times by ending the test (Step 11) and re-starting the test (Step 4). • 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.

1 of 2

Table 72: DS1 span troubleshooting *2 of 2*

Displayed Field	Function	Indication
Bit Error Count	Cumulative count of detected errors	If there are no wiring problems, the counter remains at 0. A count that pegs at 65535 or continues to increment by several hundred to several thousand on each **`list measurement`** command execution may indicate: • Intermittent or corroded connections • Severe crosstalk • Impedance imbalances between the two conductors of the receive pair or the transmit pair. Wiring may need replacement. 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.
		2 of 2

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 437 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 437 and Configurations without a Smart Jack on page 442.

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 73.

Table 73: 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 106: Network Interface at Smart Jack on page 439) 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 434. 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 106: Network Interface at Smart Jack

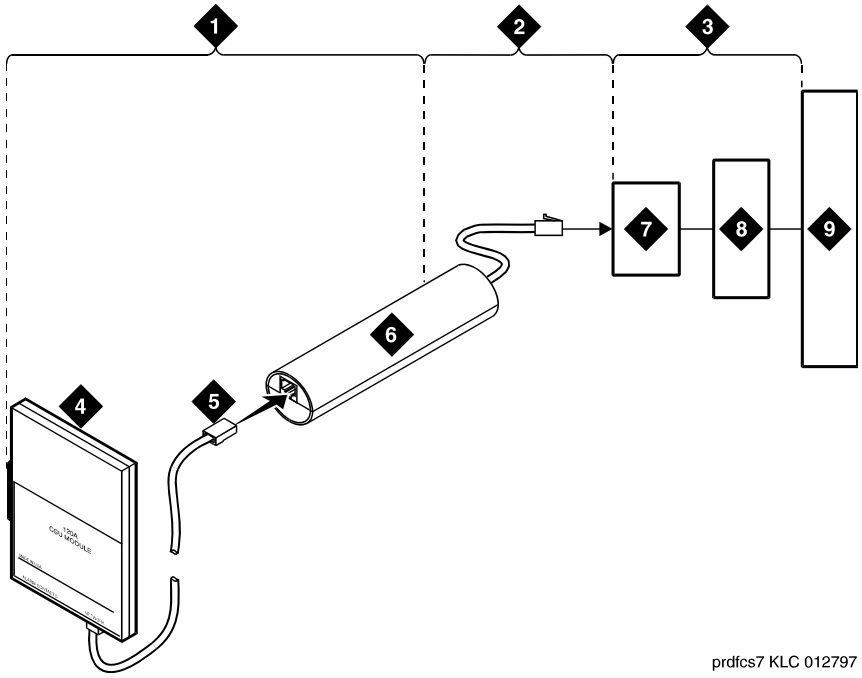


Figure notes:

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 107: Network Interface at Extended Demarcation Point (Smart Jack inaccessible)

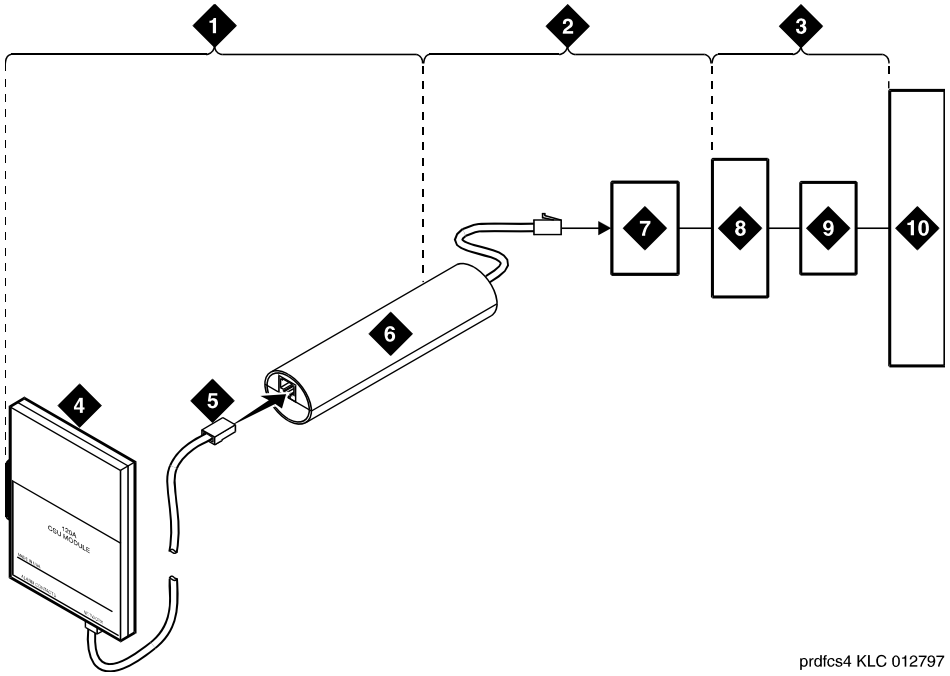


Figure notes:

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 108: Network Interface at Extended Demarcation Point (Smart Jack accessible)

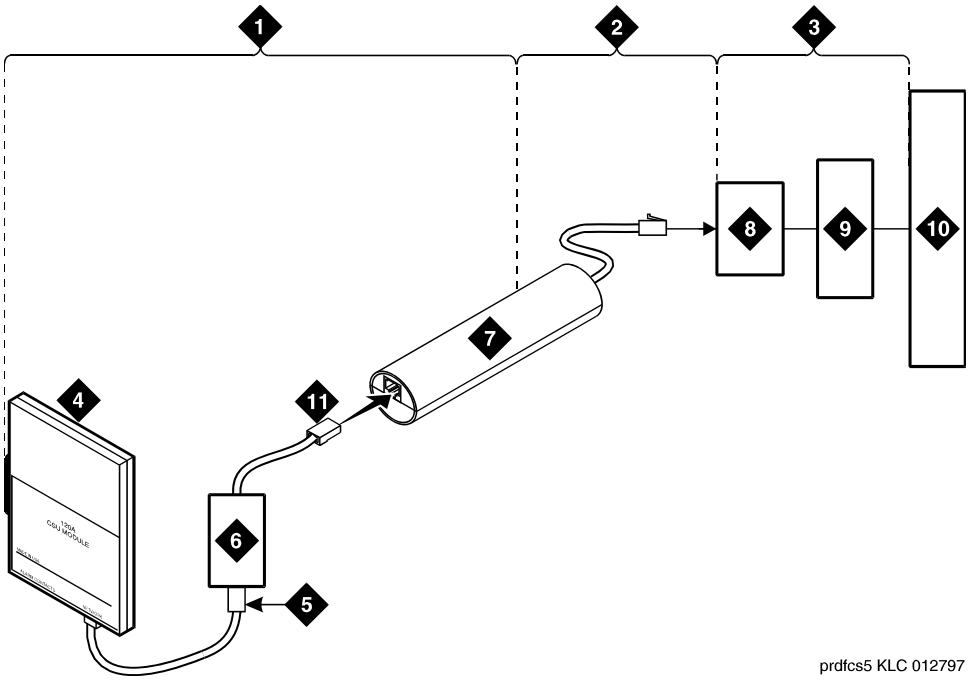


Figure notes:

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 109: Network Interface at “Dumb” Block on page 442 and Figure 110: Network Interface at “Dumb” Block with repeater line to Fiber MUX on page 443. These sections are described in Table 74.

Table 74: 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 109: Network Interface at “Dumb” Block

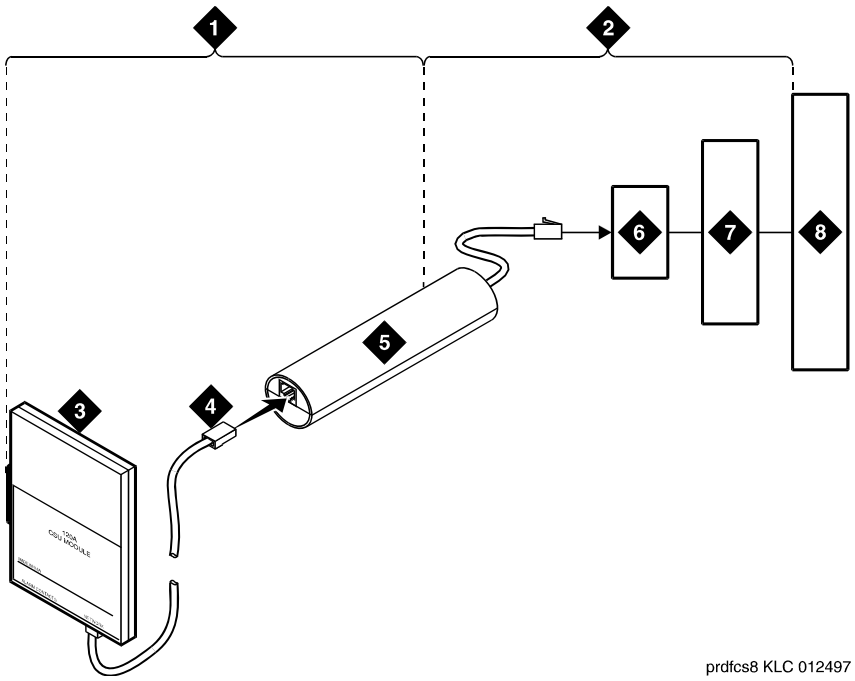


Figure notes:

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 110: Network Interface at “Dumb” Block with repeater line to Fiber MUX

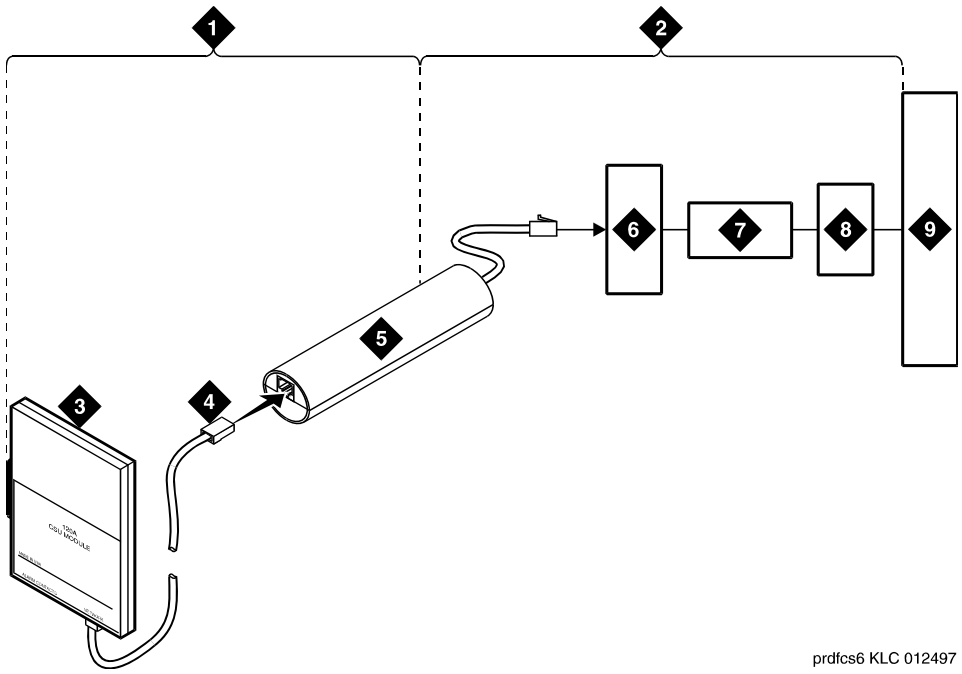


Figure notes:

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 109: Network Interface at “Dumb” Block on page 442) from the ICSU to the loopback jack as described in DS1 span test on page 434.

2. Test the loopback jack-to-dumb block and dumb block-to-CO wiring (Span Section 2 in Figure 109: Network Interface at “Dumb” Block on page 442). 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 106: Network Interface at Smart Jack on page 439
- Figure 107: Network Interface at Extended Demarcation Point (Smart Jack inaccessible) on page 440

- Figure 108: Network Interface at Extended Demarcation Point (Smart Jack accessible) on page 441
- Figure 109: Network Interface at “Dumb” Block on page 442.

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 291.

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 | 8710**: 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. **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 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 (MM711/714), 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.

4. 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, 03-300468*.

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

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

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 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 (**TTR**s). 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, 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)
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).

1 of 2

If you get...	Then...
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.
	2 of 2

Note:

For a definition of call progress tones, refer to *Overview for Avaya Communication Manager, 03-300468*.

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 451.

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 75: TDM Bus time slot numbers on page 450.
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 75.

Note:

For a definition of call progress tones, refer to *Overview for Avaya Communication Manager, 03-300468*.

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`** displays 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 75: TDM Bus time slot numbers *1 of 2*

TDM Bus A time slot	TDM Bus B time slot	Tone heard
000	256	Reorder
001	257	Reorder
002	258	Reorder
003	259	Reorder
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

1 of 2

Table 75: TDM Bus time slot numbers *2 of 2*

TDM Bus A time slot	TDM Bus B time slot	Tone heard
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 Table 76.
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, 03-300468*.

Table 76: System tone identification numbers *1 of 4*

Number	Description
00	Null tone
01	Dial tone
02	Reorder tone
03	Alert tone

1 of 4

Table 76: System tone identification numbers *2 of 4*

Number	Description
04	Busy tone
05	Recall dial tone
06	Confirmation tone
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

2 of 4

Table 76: System tone identification numbers *3 of 4*

Number	Description
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
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

3 of 4

Table 76: System tone identification numbers *4 of 4*

Number	Description
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
	4 of 4

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) might 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.

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|8710). 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.

status ip-network-region form

The **IP Network Region** form shows statistics on the Call Admission Control- Bandwidth Limitation feature. The following two figures show two different command options. The **status ip-network-region *n*** command is shown in Figure 111: status ip-network-region n on page 459. 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 111: 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, use the **status ip-network-region *n/m*** command (see Figure 112: status ip-network-region 2/3 on page 459) that 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 112: 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
```

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). **Note:** This log is cleared at midnight, server time. Use the **`display events`** command and set the **Category** field to **denial** to see the Denial Events log.

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 77 lists call processing features impacted by CAC-BL.

For more information about Call Admission Control, see the *Administrator Guide for Avaya Communication Manager, 03-300509*.

Table 77: 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 462.

  or

- Simplex mode test procedure on page 468.

E&M mode test procedure

To test the E & M mode:

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 378.
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 113: Trunk Group form on page 463 and Figure 114: Trunk Group form - E & M mode (Page 2 of 2) on page 464 show an example of the Trunk Group form.

Note:

Some field locations show below might differ from those on your system.

Figure 113: Trunk Group form

```
display trunk-group 10                                          Page  x of  x

                                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 114: Trunk Group form - E & M mode (Page 2 of 2)

```
                                                          Page x of  x

                                  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 78: Carrier lead appearances MDF *1 of 3*

110 connecting block terminals	CO Trunk TN747	Tie Trunk TN760
1	T1	T1
2	R1	R1
3		T11
4		R11

1 of 3

Table 78: Carrier lead appearances MDF *2 of 3*

110 connecting block terminals	CO Trunk TN747	Tie Trunk TN760
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	
26	R5	
27		
28		
29		
		2 of 3

Table 78: Carrier lead appearances MDF *3 of 3*

110 connecting block terminals	CO Trunk TN747	Tie Trunk TN760
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		

3 of 3

Simplex mode test procedure

To test using the simplex mode:

1. Repeat steps 1 through 7 of the **E&M mode test procedure** on page 462.
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 115 shows page 2 of the Trunk Group form.

Figure 115: 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 462.

TN760E tie trunk option settings

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 79: Signaling Formats for TN760E on page 470 and Table 80: Signaling type summary on page 470), set the switches on the TN760E and administer the port using Figure 116: TN760E tie trunk circuit pack (component side) (R758183) on page 471 and Table 81: TN760E option switch settings and administration on page 471.

Table 79: 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 80: 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
Type I Compatible	Open1/ battery	Ground	Ground	Open1/ battery
Type V	Open1/ battery	Ground	Open	Ground
Type V Reversed	Ground	Open	Ground	Open

1. An open circuit is preferred instead of battery voltage.

Figure 116: TN760E tie trunk circuit pack (component side) (R758183)

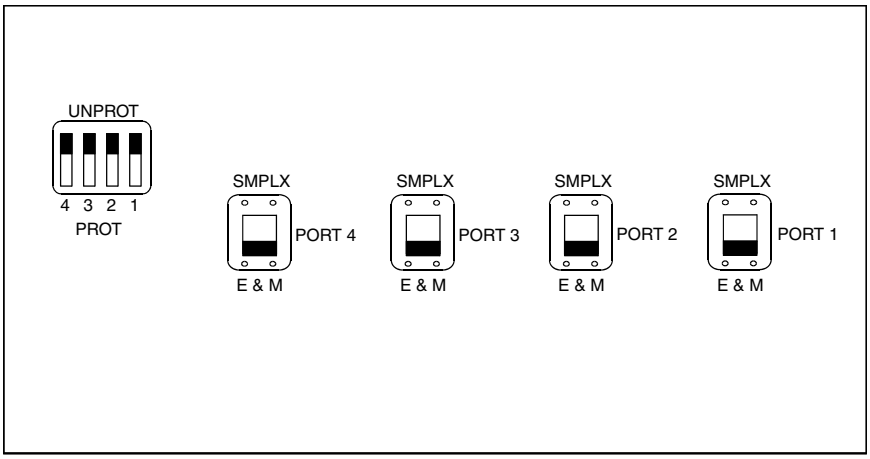


Table 81: TN760E option switch settings and administration

Installation situation		Preferred signaling format		E&M/SMPLX switch	Prot/Unprot switch	Administered port
Circumstance	**To**	**System**	**Far-End**			
Co-Located	Avaya PBX	E&M Type 1 Compatible	E&M Type 1 Standard	E&M	Unprotected	Type 1 Compatible
Inter-Building	Avaya PBX	Protected Type 1 Compatible	Protected Type 1 Standard Plus Protection Unit	E&M	Protected	Type 1 Compatible
Co-Located	Net Integrated	E&M Type 1 Standard	Any PBX	E&M	Unprotected	Type 1

TN464E/F option settings

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 82 and Figure 117.

Table 82: 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 117: TN464E/F option settings

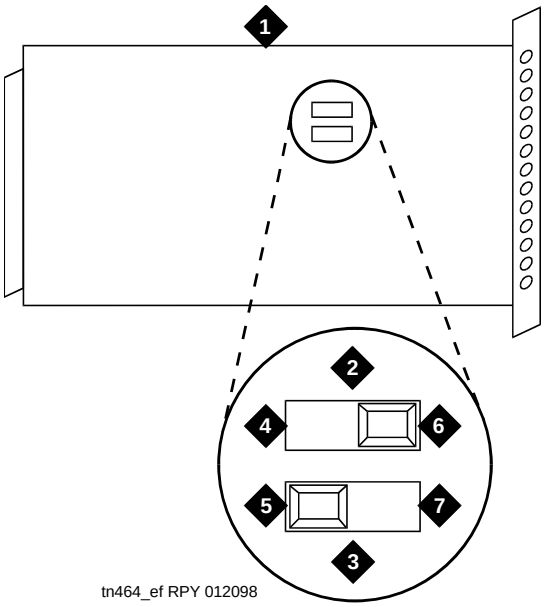


Figure notes:

1. Backplane connectors
2. 24/32 channel selector
3. 75/120 Ohm selector
4. Faceplate
5. 32 channel
6. 120 Ohm (shown selected)
7. 24 channel (shown selected)

Terminating Trunk Transmission testing

Note:

The capability described in this section is not available on S8300 server configurations.

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 51 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 G250 / G350 Media Gateways

To remove or restore power:

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 (03-300430)*.

   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 / restoring power: S8700 Series Media Servers

Always shut down the Avaya S8700 Series media servers from the Maintenance Web Interface to ensure that all active processes terminate properly.

Maintenance activity places different demands on power-removal scenarios. You can busy-out and remove power from the Off Line (standby) server to replace components, replace the entire server, or relocate the server. For planned power outages, you can shut down both servers sequentially. Choose from these procedures:

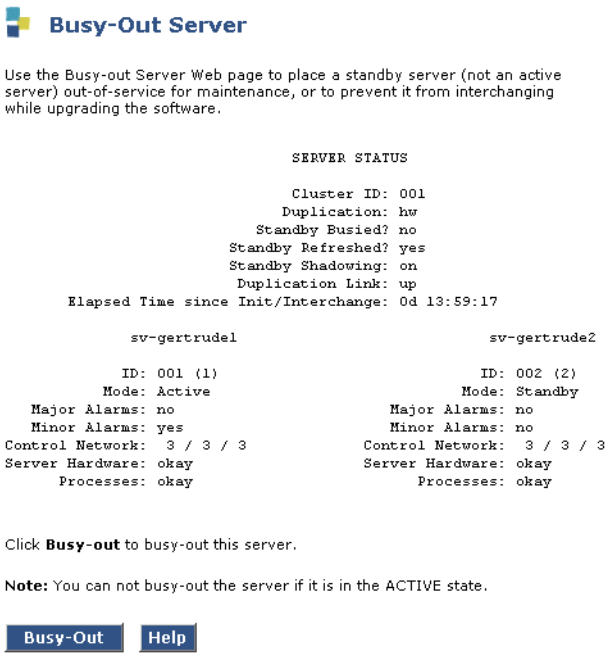
- Shutting down the Off Line (standby) server
- Shutting down the server pair
- Restoring power to the S8710 or S8720 media servers

Shutting down the Off Line (standby) server

To shut down a S8710 or S8720 Off Line (standby) media server for maintenance:

1. At the Web interface's main menu for the Off Line (standby) server select **Data Backup/ Restore > Backup Now** and backup the data to flashcard.
2. Select **Server > Busy-out Server** from the main menu.

   The **Busy-out Server** page displays.



3. Ensure that you are on the Off Line (standby) server and click on **Busy-Out**.

Note:

You cannot busy-out the On Line (active) server, and while the Off Line (standby) server is busied-out, server interchange cannot occur.

4. Select **Shutdown Server** from the main menu.

   The **Shutdown This Server** page displays.

5. Select **Immediate Shutdown** and uncheck (deselect) **Restart server after shutdown**.
6. Press the **Shutdown** button and wait until the server has powered down.
7. When both server has powered down, remove the power.
8. To restore power see Restoring power to the S8710 or S8720 media servers on page 477.

Shutting down the server pair

Note:

This procedure shuts down both servers and terminates Avaya Communication Manager, meaning that the entire phone system is inoperable including Emergency Transfer. Users cannot make any phone calls

To shut down both the On Line (active) and Off Line (standby) servers:

1. At the Web interface's main menu for the Off Line (standby) server select **Data Backup/ Restore > Backup Now** and backup the data to flashcard.

2. Select **Shutdown Server** from the main menu.

   The **Shutdown This Server** page displays.

3. Select **Immediate Shutdown** and uncheck (deselect) **Restart server after shutdown**.
4. Press the **Shutdown** button and wait until the server has powered down.
5. At the Web interface's main menu for the On Line (main) server select **Backup Now** and backup the data to flashcard.
6. Select **Shutdown Server** with these options:
   - Choose the **Immediate** option.
   - Select **Even If Server is Active**.
   - Do not select **Restart server after shutdown**.
7. Click the **Shutdown** button and wait until the server has powered down.
8. When both servers are powered down, remove power from the servers.
9. To restore power see Restoring power to the S8710 or S8720 media servers on page 477.

Restoring power to the S8710 or S8720 media servers

To restore power to the S8710 or S8720 server:

1. Apply power to the server by plugging the cable into the appropriate power source and into the rear connector of the server.
2. Push the power button on the front panel of the server.

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 118: Setting the neon voltage on page 479.)

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.

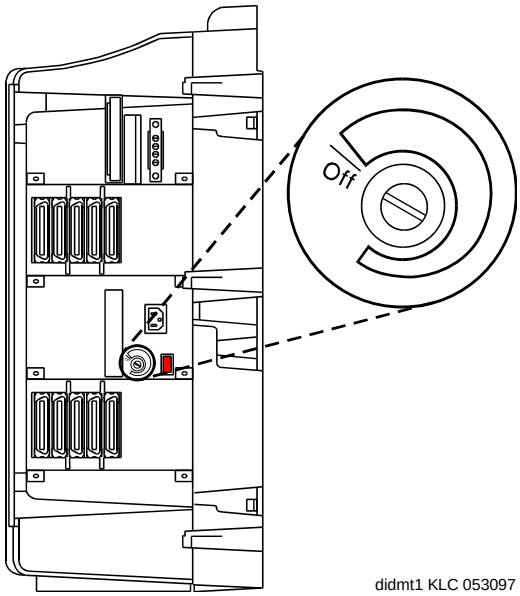
Use the following procedure to adjust the neon voltage:

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 118: Setting the neon voltage on page 479.

   Ensure that the message lamp still lights when the adjustment is finished.
4. Type **`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 118: 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 ATMS summary report on page 489 or ATMS detail report on page 490.

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. These tests are not useful in every environment, and the trunk test parameters must be met, otherwise Test #844-848 Transmission Test aborts with Error Code 1005 for these unsupported trunk groups:

- ISDN-PRI
- SIP
- DID
- Any incoming trunk group (transmission tests can only be run on outgoing trunks)

For ATMS tests to run, several administrative prerequisites must be met. Table 83 shows the field entries necessary to enable testing.

Table 83: ATMS administration *1 of 2*

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	***UUCSS01***, where UUCSS is the location of any TN771
	Port Type COR	105TL. The number of a COR that has testing enabled

1 of 2

Table 83: ATMS administration *2 of 2*

Form	Field	Entry/Remarks
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
		2 of 2

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. Table 84 shows which tests are run for each type of TTL.

Input parameters

Table 84: Input parameters (analog test call)

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 484. 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. “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 483.

Different TTLs have different measurement capabilities, and you will need the information about specific TTL types in Table 85, which does not include the self-test nor does it distinguish between measurements for different test tone levels.

Table 85: 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 (03-300430)*.
- 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 487. 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 119 shows a typical result for **`test analog-testcall trunk 60`**.

Figure 119: 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
```

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.

1 of 2

Field	Description
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. • 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. • 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 (03-300430)*.

2 of 2

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 486 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.

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.
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.

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 120 shows a typical summary report.

Figure 120: ATMS 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
```

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.

1 of 2

Field	Description
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.

2 of 2

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 121: ATMS detail report on page 490). 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 121: 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
```

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
Tst Rslt	The results of the trunk transmission test as follows: ● pass: the test call completed successfully and trunk performance was satisfactory. ● marg: trunk measurements exceeded the marginal threshold, but not the unacceptable. ● fail: trunk measurements exceeded the unacceptable threshold. ● 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 (03-300430)*. ● 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.

1 of 2

Field	Description
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 (slot number) of an MM stratum clock source. For the MM720/MM722 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 sync source 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 86: 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 87: 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 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 88: 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 89:

Table 89: 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 90: 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 91: 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 92: 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 93: 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 94: 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 95: IP Telephone problems and solutions on page 498 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 95: IP Telephone problems and solutions *1 of 3*

Problem/Symptom	Suggested solution
Phone does not activate after connecting it the first time	Unless your System Administrator has already initialized your telephone, you may experience a delay of several minutes before it becomes operational. Upon plug-in, your telephone immediately begins downloading its operational software, its IP address and any special features programmed by your System Administrator from the server to which it is connected. Report any delay of more than 8-10 minutes to your System Administrator.

1 of 3

Table 95: IP Telephone problems and solutions *2 of 3*

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

2 of 3

Table 95: IP Telephone problems and solutions *3 of 3*

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

3 of 3

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 96:

Table 96: Resetting the IP Telephone

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

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

   Note:

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

Numerical

120A ICSU 437
3-in-24 pattern 435

A

ACA, see Automatic Circuit Assurance
access
  CLI navigation 94
  Communication Manager 53
  log in methods 90
  physical connections 69
  remote 53
  telnet 53
  via Avaya Site Administration 53
  via Avaya stack IP address 53
  via serial cable 53
accessing the server 122
adding
  local logins 98
  MPC remote (modem) logins 98
administration
  shuffling and hairpinning maintenance 252
admonishments 15
air filters 379
air filters, inspecting 379
alarm logs 26
Alarm Reporting Options form 31
alarms
  classifications 29
  external leads 35
  logs 26
  maintenance objects (MOs) 28
  notification
    and ASA 16
  reporting
    Alarm Reporting Options form 31
American National Standards Institute, see ANSI
analog
  carrier signal 38
  modem transmission 39
  port, insertion loss 45
Analog Media Module 57
analog trunk/telephone port board Media Module . . 52
analog-to-
  analog
    echo path delay 47
    frequency response 44
    intermodulation distortion 45
    peak noise level 47
    quantization distortion loss 46
  digital
    coder/decoder 39
    frequency response 44
    intermodulation distortion 45
    peak noise level 47
    quantization distortion loss 46
ANSI 44
application protocols 47
ARB (Arbiter) Linux process 126
ASAI
  troubleshooting 288
ASG
  log entries 343
Asynchronous Data Unit (ADU)
  proprietary signal 39
ATMS 481
Auto Fallback to Primary 138
Automatic Circuit Assurance (ACA) 283
automatic launch of trace-route 127
Avaya S8300 Media Server with G700 Media Gateway
  access 53
  maintenance features 66
Avaya Site Administration 53

B

background tests 27
  fixed interval 27
  scheduled 27
backup and restore
  Web Interface 53
backup/restore 341
basic input/output system, see BIOS
batteries
  preventive maintenance 455
BIOS 125
bit rate
  setting 472
BIU, replacing 383
boot timeout
  disabling through MPC interface 118
  disabling with Linux commands 119
Busy Verification of Terminals and Trunks 284

C

cabling
DS1 connectors . . . 303
capabilities, system . . . 36-47
caution symbol . . . 15
CEPT1 . . . 39
changing
local login to remote login . . . 99
remote login to local login . . . 99
character code, 8-bit . . . 39
characteristics, transmission . . . 44-47
check server status
Web Interface . . . 53
circuit packs
and electrostatic discharge (ESD) . . . 16
DS1 CONV . . . 379
packet-bus failures . . . 390
replacing . . . 378
requiring special procedures . . . 378
reseating . . . 378
TN572 . . . 379
TN573 . . . 379
TN750 . . . 379
using the packet bus . . . 389
CLI
G700 . . . 54
G700 commands . . . 50
Layer 2 Switching Processor . . . 54
navigational aid . . . 94
codec . . . 39
coder/decoder, analog-to-digital, see codec
codes
service . . . 48
cold restarts . . . 220
cold starts
with translations loading . . . 221
command
userlock . . . 344
command line interface
logged entries . . . 348
Command Line Interface Help . . . 92, 93
commands
set tone-clock . . . 408
to diagnose packet-bus problems . . . 403
Communication Manager . . . 52
maintenance features . . . 66
Communication Manager application
initializing . . . 126
Conference, Transfer, and Call-Forwarding denial . . . 43
connecting to the MPC . . . 99
Connection Preserving Failover/Failback . . . 138
feature interactions . . . 146
Final Cleanup Timer (FCT) . . . 144
timers . . . 143
VoIP monitoring . . . 142
connectivity
ISDN-BRI/packet bus . . . 288
packet bus . . . 388
rules . . . 41
CO-trunk-to-digital interface frequency response . . . 44

D

danger symbol . . . 15
data
communications equipment, see DCE
service unit . . . 38
terminal equipment . . . 36
data-link layer, OSI . . . 36
DC power
signaling leads . . . 470
DCE . . . 36
D-channel
protocol . . . 36
DCP . . . 38
DCP Media Module . . . 52, 59
delay, echo path . . . 47
demand tests . . . 28
detecting MPC . . . 275
Digital
Multiplexed Interface (DMI) . . . 39
Signal Level 1 (DS1) . . . 39
digital
port, insertion loss . . . 45
to analog
peak noise level . . . 47
quantization distortion loss . . . 46
to digital
echo path delay . . . 47
disable
boot timeout through MPC interface . . . 118
boot timeout with Linux commands . . . 119
Disconnect Supervision . . . 42
distortion
intermodulation . . . 45
quantization loss . . . 46
Downloading new firmware from the Web to the staging area . . . 122
DS0 Loop-Around Test Call . . . 447
DS1 . . . 66
cable connectors . . . 303
DS1 CONV
circuit packs . . . 379
loopbacks . . . 303

DS1 Media Module
synchronization . . . 493
DS1 span . . . 432, 433
troubleshooting . . . 435
DSO frequency response . . . 44
DSU, see Data Service Unit
DTE, see data terminal equipment
DTMR Test Call . . . 448
duplication
of servers
spontaneous interchanges . . . 295

E

E1/T1 Media Module . . . 52
tests . . . 60
echo
path delay . . . 47
return loss . . . 47
EIA . . . 44
Electronic Industries Association, see EIA
electrostatic discharge (ESD), circuit packs . . . 16
Enterprise Survivable Server . . . 138
Enterprise Survivable Servers
traceroute command . . . 129
ERL, see echo-return loss
error logs . . . 26
errors
control . . . 36
logs . . . 26
hardware . . . 29
reporting, maintenance objects (MOs) . . . 28
ESD, See electrostatic discharge
European conference of postal/ telecom rate 1, see CEPT1
expansion interface (EI)
manual loop-back procedure . . . 301
expansion port networks, see port networks (PNs)

F

Facility Interface Code . . . 48
Facility Test Calls . . . 445
failed IP network region connections . . . 256
failed ip-network-regions, testing . . . 256
fault isolation . . . 50
FCC . . . 48
feature capacities . . . 36-47
Federal Communications Commission, see FCC
fiber
fault-isolation procedure . . . 296
FIC, see Facility Interface Code
field replaceable components . . . 50
file monitoring
Tripwire . . . 350
filters
air filter . . . 375
firewall
logged entries . . . 346
firmware
upgrading . . . 123
upgrading MPC . . . 121
firmware upgrades . . . 53
firmware version
determining latest . . . 121
flow control . . . 36
forms
Alarm Reporting Options, setting . . . 31
frequency response
analog-to-analog . . . 44
analog-to-digital . . . 44

G

G250
Standard Local Survivability . . . 138
G700
administration . . . 50
CLI . . . 54
CLI commands . . . 50
DS1 synchronization . . . 493
maintenance . . . 50
status functions . . . 50
synchronization . . . 493
viewing sync sources . . . 495
G700 Media Gateway
system reset . . . 223
unexecuted tests . . . 63
G700 Media Server
tests . . . 67
unexecuted tests, TDM bus . . . 65
unexecuted tests, tone detector . . . 64
unexecuted tests, tone generator . . . 64

H

H.248 link recovery . . . 149
H.323 trunks, troubleshooting . . . 250
hardware sanity
device . . . 126
hmm Linux process . . . 126
hot swap . . . 52
S8300 caution . . . 52

I

impedance, setting . . . 472
impedances
loop in . . . 47
termination . . . 47

initialization
active server . . . 126
and recovery . . . 125
arbiter module . . . 126
Communication Manager application . . . 126
hardware-sanity check . . . 126
init process . . . 125
server . . . 125
standby server . . . 127
watchdog process . . . 126
initmap process . . . 126
insertion loss . . . 45
installing a BIU or rectifier . . . 384
interchanges
commands
reset pnc interchange . . . 408
reset system interchange . . . 408
interface
physical . . . 38
intermodulation distortion . . . 45
internal link
verifying . . . 118
intervening switching systems . . . 41
inventory data . . . 117
IP connection status
station . . . 253
trunk . . . 254
IP events
logged entries . . . 347
IP events logs . . . 340
ip network region status . . . 255
IP softphones, troubleshooting . . . 260
IP telephone, troubleshooting . . . 260
IP telephones
error message . . . 499
headset/handset distortions . . . 499
inoperable speakerphone . . . 500
no activation . . . 498
no characters . . . 499
no dial tone . . . 499
no ring . . . 500
possible problems . . . 498
power cycle . . . 501
reset procedures . . . 500
solutions . . . 498
ISDN . . . 66, 67
BRI definition . . . 38
D-channel treatment . . . 36
PRI definition . . . 38
ISDN-BRI
troubleshooting . . . 288
ISDN-PRI
troubleshooting . . . 284

J

jacks, network . . . 48

L

Layer 2 Switching Processor
CLI . . . 54
layers, of OSI model
and related protocols . . . 38
LEDs . . . 66
and
electrostatic discharge (ESD) . . . 16
link recovery . . . 149
administration . . . 154
feature interactions . . . 157
link loss delay timer . . . 154
mgc list . . . 156
network fragmentation . . . 158
primary search timer . . . 156
total search timer . . . 156
transition point . . . 156
Linux
commands
statapp . . . 126
kernel . . . 125
loader . . . 125
processes
hmm . . . 126
scripts
rc . . . 125
service startup . . . 125
local connections to the MPC through SSH . . . 101
local connections to the MPC through the browser . . . 99
local connections to the MPC using PuTTY . . . 101
Local Survivable Processor
traceroute command . . . 129
logged logins . . . 342
logging in to the MPC . . . 99
logging in to the MPC locally through SSH . . . 101
logging in to the MPC locally through the browser . . . 99
logging in to the MPC remotely through SSH . . . 101
logging in to the MPC remotely through the browser 102
logging in to the SAMP locally using PuTTY . . . 101
login lockout timer . . . 342
login procedures . . . 90
logins
adding MPC logins . . . 97
changing local login to remote login . . . 99
changing remote login to local login . . . 99
local . . . 98
MPC remote (modem) . . . 98
removing from MPC . . . 99

loop input impedances 47
loopback tests
fiber fault-isolation procedure 302
loopbacks
DS1 CONV 303
DS1 CONV tests 303
loss
echo return 47
insertion 45
quantization distortion 46
single-frequency 47

M

maintenance
arenas 50
background testing 27
packet bus 391
preventive 455
maintenance features
Avaya S8300 Media Server with G700 Media Gateway 66
Communication Manager 66
maintenance objects (MOs)
alarms 28
defined 25
error conditions 28
maintenance tasks 13
maintenance users 14
Maintenance Web Interface
current alarms 342
master boot record (MBR) 125
media gateway controller list 138
Media Module
adding 52
allowable tests 56
DCP 59
DEFINITY-equivalent elements 54
E1/T1 52
hot swap 52
invalid tests 56
maintenance 52
removing 52
replacing 52
tests 66, 67, 68
voice announcement 62
VoIP 52
Media Modules
Analog Media Module 57
analog trunk/telephone port board 52
DCP 52
E1/T1 60
MGP CLI 54
mismatch of signals 42
MOs, see maintenance objects (MOs) 29
MPC
adding
logins 97
connecting to 99
logging in 99
login administration 97
overall system health 111
rebooting 282
MPC interface
home page 104
Multimedia Interface (MMI) 49

N

Neon voltage 478
network interface 437
network jacks 48
network recovery
timers 137
Final Cleanup Timer (FCT) 138
Link Loss Delay Timer (LLDT) 138
No Service Timeout Timer (NSTT) 138
Primary Search Timer (PST) 138
Total Search Timer (TST) 138
noise, peak level 47
notification, of
alarms
and ASA 16

O

Open System Interconnect model 36
Layer 1 (physical layer) 36
protocols 38
Layer 2 (data-link layer) 36
protocols 39
OSI model, see Open System Interconnect model

P

packet bus
and circuit-pack failures 390
circuit packs 389
connectivity 388
correcting faults 407
definition 387
fault isolation 402
faults 387
in duplicated systems 408
ISDN-BRI connectivity 289
maintenance 391
repair 385
reset pnc interchange 408
reset system interchange 408

packet bus, (continued)
set tone-clock . . . 408
TDM-bus comparison . . . 392
troubleshooting . . . 404, 409
parts, field replaceable . . . 50
password protection . . . 120
PBX standard, RS-464A . . . 44
PCD process . . . 127
PCM-encoded analog signal . . . 39, 42
peak noise level . . . 47
performance . . . 36-47
echo-return loss . . . 47
single-frequency return loss . . . 47
physical layer, OSI . . . 36
port networks (PNs)
troubleshooting packet bus . . . 415
port-to-port insertion loss . . . 45
power
adding . . . 479
distribution units . . . 455
interruptions . . . 34
removing . . . 474, 479
restoring . . . 474
power cord . . . 479
power shutdown
G250 / G350 Media Gateways . . . 474
Shutting down the S8710 / S8720 server pair . . . 476
Shutting down the standby server . . . 475
preventive maintenance . . . 455
batteries . . . 455
PRI . . . 38
private-line service codes . . . 48
procedures
SNI/EI manual loop back . . . 301
Process Manager (prc_mgr) . . . 126
protocols
8-bit character code . . . 39
ADU . . . 39
analog . . . 38
BRI . . . 38
CEPT1
DCP . . . 38
Digital Multiplexed Interface . . . 39
for applications . . . 47
in layers of OSI model . . . 38
PRI . . . 38
summary of states . . . 40
system . . . 36
voice-grade data . . . 39
PuTTY
using to log in to the SAMP locally . . . 101

Q

quantization distortion loss . . . 46

R

rc Linux script . . . 125
rear panel connector . . . 48
rebooting the MPC . . . 282
reboots
reset level 4 . . . 222
rectifier, replacing . . . 383
remote connections to the MPC through SSH . . . 101
remote connections to the MPC through the browser . . . 102
removing
login from MPC . . . 99
REN, see ringer equivalency numbers
reports . . . 353
reset
levels
1 (warm restarts) . . . 219
2 (cold-2 restarts) . . . 220
4 (reboots) . . . 222
SAT commands
reset pnc interchange . . . 408
reset system interchange . . . 408
reset commands
reset system 3
cold starts . . . 221
reset system 5
DEFINITY extended reboot . . . 223
resets, system . . . 223
Restoring power
S8710 / S8720 servers . . . 477
ring ping . . . 478
ringer equivalency numbers . . . 48
rootkit . . . 337
RS-232
interface . . . 38
RS-449
physical interface . . . 38
RS-464A . . . 44
rules, connectivity . . . 41
run-on-standby processes . . . 127

S

S8300
disk parking . . . 52
S8300 Media Server
hot swapping caution . . . 52
shutdown . . . 52
safety labels . . . 15
SAT . . . 50
SAT commands
status port-network . . . 407
searching log entries . . . 349

security
system intrusion . . . 337
serial cable . . . 53
servers
duplicated, troubleshooting . . . 295
initialization . . . 125
software/firmware modules . . . 125
service codes . . . 48
set options command . . . 31
set SAT commands
set tone-clock . . . 408
setting
bit rate . . . 472
line impedance . . . 472
neon voltage . . . 478
SFRL, see single-frequency return loss . . . 47
shadowing, between servers . . . 127
shuffling and hairpinning, maintenance administration . . . 252
signaling leads, DC power . . . 470
signals
mismatch . . . 42
PCM-encoded analog . . . 42
single-frequency return loss . . . 47
smart jack
configurations . . . 437
SNI
manual loop-back procedure . . . 301
software
upgrades . . . 53
software updates
logged entries . . . 345
specifications . . . 36-47
spontaneous interchanges . . . 295, 296
SSH & SFTP
symmetric algorithms . . . 84
SSH & SFTP protocols
TN2312AP/BP (IPSI) . . . 84
TN2501AP (VAL) . . . 84
TN2602AP (Crossfire) . . . 84
TN799DP (CLAN) . . . 84
Standard Local Survivability (G250) . . . 138
Standard Local Survivability (SLS)
supported functionality . . . 178
startup Linux scripts . . . 125
statapp Linux command . . . 126
station
to CO trunk, frequency response . . . 44
to digital interface, frequency response . . . 44
to station, frequency response . . . 44
status
Linux commands
statapp command . . . 126
port-network . . . 407
SAT commands . . . 403
status, ip network region . . . 255
summary of protocol states . . . 40
switch
transmission characteristics . . . 44-47
switch settings
TN464 circuit pack . . . 472
TN760 tie trunk . . . 470
synchronization . . . 36
commands . . . 495
local . . . 497
primary . . . 497
secondary . . . 496
viewing sources . . . 495
system
insertion loss . . . 45
protocols . . . 36
quantization distortion loss . . . 46
specifications . . . 36-47
System Access Terminal . . . 53
system intrusion . . . 337
firewall settings . . . 346
interpreting Tripwire reports . . . 353
logging root access . . . 343
sniffer . . . 337
Tripwire . . . 350
warning signs . . . 337
system logs . . . 339
system resets . . . 223
System Tone Test Call . . . 452

T

T1 . . . 432
TDM bus
packet bus comparison . . . 392
time slots . . . 450
TDM Bus Time Slot Test Call . . . 449
technical specifications . . . 36-47
telecommuter application . . . 260
terminal
equipment port wiring . . . 48
terminal emulation
ntt . . . 82
w2ktt . . . 82
Terminating Trunk Transmission (TTT) test . . . 470
termination impedances . . . 47
test calls
DS0 loop around . . . 447
DTMR . . . 448
facility . . . 445
system tone . . . 452
TDM bus time slot . . . 449
tone receiver . . . 448
trunk . . . 446

testing
analog tie trunk back-to-back . . . 456
background . . . 27
demand . . . 28
fiber fault isolation . . . 302
Media Module . . . 56
testing failed ip-network-regions . . . 256
testing HPI . . . 278
testing internal LAN . . . 276
testing MPC through SSH . . . 278
testing NTP . . . 281
tests
tone detector, unexecuted . . . 64
unexecuted, G700 . . . 63
unexecuted, TDM bus . . . 65
unexecuted, tone generator . . . 64
tests and audits
DS1 Span test . . . 434
tie trunk
circuit pack option settings . . . 470
time slots
TDM bus . . . 450
timers
Final Cleanup Timer (FCT) . . . 144
Watchdog
hardware timer . . . 126
TN464 circuit pack
option settings . . . 472
TN572 circuit packs . . . 379
TN573 circuit packs . . . 379
TN750 circuit packs . . . 379
TN760 circuit pack
option settings . . . 470
tones
system tone identification numbers . . . 452
trace-route . . . 127
traceroute
interpreting the Web interface logs . . . 132
Transfer on Ringing . . . 43
transmission
characteristics . . . 44-47
errors . . . 36
stream . . . 36
Tripwire . . . 350, 353
log entries . . . 343
policy file . . . 350
troubleshooting . . . 13
ASAI problems . . . 288
detecting MPC . . . 275
duplicated media servers . . . 295
IP softphones . . . 260
IP telephones . . . 260, 498
ISDN-
BRI problems . . . 288
PRI
endpoints (wideband) . . . 286
test-call problems . . . 291
outgoing ISDN-testcall command . . . 294
packet bus . . . 404, 409
S8400 MPC . . . 275
testing HPI . . . 278
testing internal LAN . . . 276
testing MPC through SSH . . . 278
testing NTP . . . 281
troubleshooting H.232 trunks . . . 250
trunk
speed . . . 42
test call . . . 446
trunking
facilities . . . 41
TTT, see Terminating Trunk Transmission

U

UPS . . . 34

V

V.35, DTE-to-DCE interface . . . 38
voice announcement Media Module
tests . . . 62
voice-grade data . . . 39
VoIP Media Module . . . 52

W

warm restarts (reset level 1) . . . 219
warning symbol . . . 15
Watchdog
processes
server-initialization process . . . 126
Web browser requirements . . . 97
web interface . . . 50
wiring
premises . . . 48
terminal equipment ports . . . 48