Maintenance Procedures for Communication Manager, Branch Gateways and Servers

Release 6.2
03-300432
Issue 8
July 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Third Party Components

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

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

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

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

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

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

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

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

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

Means of Connection:

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

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

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

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

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

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

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

Installation and Repairs

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

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

FCC Part 68 Supplier's Declarations of Conformity

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

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

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

Canadian Conformity Information

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

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

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

European Union Declarations of Conformity

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

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

European Union Battery Directive

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

Japan

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Overview 13
- Audience 13
- Safety and security-alert labels 14
- Observing safety precautions 14
  - Electrostatic discharge 15
  - Suppressing alarm origination 16
- Related resources 17
  - Documentation 17

Chapter 2: Maintenance strategy 21
- Maintenance objects 21
- Maintenance testing 22
  - Background testing 22
  - Demand testing 23
- Alarm and error reporting 24
  - Alarm and error logs 24
  - Alarm reporting 25
  - Alarm reporting options 25
- Power interruptions 28
  - Nominal power holdover 28
  - Power interruption effects 29
  - External alarm leads 29
  - Communication Manager Messaging 30
- Protocols 32
  - Open Systems Interconnection model 32
  - Protocol usage 34
  - Protocol states 35
  - Connectivity rules 36
- Signaling 37
  - Disconnect supervision 37
  - Transmission characteristics 39
- Service codes 42
- Facility Interface Codes 43
  - Facility Interface Codes list 43
- Multimedia Interface 44
- Maintenance of G430 Branch Gateway and G450 Branch Gateway and servers 44
  - Maintenance Web Interface 45
  - Avaya G450 Branch Gateway and G430 Branch Gateway CLI 46
- G430 Branch Gateway and G430 Branch Gateway maintenance strategy with S8300D 46
  - Hot swapping media modules 47
- G450 and G430 server-controlled maintenance 48
  - Communication Manager equivalent elements 48
  - Capacity constraints and feature limitations 49
  - Maintenance features for G450 Branch Gateway and G430 Branch Gateway 57

Chapter 3: Server initialization and network recovery 61

Duplicated server initialization 61
Active server initialization 62
Standby server initialization 62
Automatic trace-route 63
Hardware and software requirements 63
Monitored links 64
Administration 65
Command results 67
Conditions and interactions 71
Network recovery 72
Recovery timers and interactions 73
Connection preserving failover and failback 75
H.248 server-to-gateway Link Recovery 77
H.323 Link Recovery 86
IP-Option System Parameter field descriptions 92
IP Network Regions field descriptions 93
H.323 Trunk Link Recovery 94
Auto Fallback to Primary 96
Survivable Remote Servers 97
Survivable Core Server 98
WAN Remoted Port Network 100
Chapter 4: General troubleshooting 103
Commonly-accessed directories and files on Linux servers 103
Identify the problem 105
Equipment indicators 106
User-reported problems 106
Checklist for resolving a user reported problem 107
Resolving a user reported problem 107
Status reports and activity tracing 110
Alarm and event logs 111
Maintenance subsystems 113
Current alarms 114
Filtering alarm report 116
Filtering event report 118
Viewing the Web interface logs 119
Communication Manager report interpretation 120
Analyzing IP Telephony problem 121
Repairing or escalating a problem 122
Illustrating a repair procedure 123
Chapter 5: Troubleshooting IP telephony 127
TN2302AP IP Media Processor or TN799DP CLAN circuit pack does not work 127
Inspecting board location 127
Administering a correct resource for a specified region 127
Inspecting administered TN799DP boards 128
H.323 trunks troubleshooting 128
Signaling group assignments 128
No MedPro resources available 129

CLAN sharing ... 130
Shuffling and hairpinning ... 130
Avaya IP telephones installation or administration is not working ... 136
IP Softphone Troubleshooting ... 138
Telecommuter use of telephone lines ... 138
iClarity audio level adjustments ... 138
No Dial Tone ... 139
Talk path ... 142
Poor audio quality ... 148
Dropped calls ... 152
Echo ... 153
Chapter 6: Troubleshooting trunks ... 155
Troubleshooting trunks with Automatic Circuit Assurance ... 155
Busy Verification of Terminals and Trunks usage ... 155
ISDN-PRI troubleshooting ... 156
Troubleshooting ISDN-PRI endpoints (wideband) ... 158
ISDN-BRI and ASAI problems ... 159
Troubleshooting ISDN-BRI and ASAI ... 164
ISDN-PRI test calls troubleshooting ... 165
Synchronous method ... 165
Asynchronous method ... 166
Test ISDN-TestCall response field descriptions ... 167
Troubleshooting outgoing ISDN-testcall command ... 167
Chapter 7: Other troubleshooting ... 169
Troubleshooting duplicated servers ... 169
Spontaneous interchange of a server ... 169
Causes of spontaneous interchange of a server ... 170
Isolating fiber link fault ... 171
Running tests for each of the fiber link's endpoints ... 173
Troubleshooting SNI/EI links with manual loop-back ... 175
Fiber faults with loopback tests isolation ... 176
DS1 interface cable connectors ... 177
Linux time and Communication Manager time ... 178
Troubleshooting problems with Linux time and Communication Manager time ... 178
Troubleshooting Network Time Server ... 180
Chapter 8: Communication Manager and Linux logs ... 181
System intrusion detection ... 181
Syslog server ... 181
Administering the syslog server ... 182
Administering logging levels in Communication Manager ... 183
Logging Levels form, page 1 field descriptions ... 184
Logging Levels form, page 2 field descriptions ... 184
Accessing system logs through the Web interface ... 185
List of system logs ... 186
Select a View ... 194
Select Event Range ... 197
Display Format ... 197

Log entries interpretation ... 198
Common timestamp interpretation ... 198
Platform bash command history log format ... 198
Reclaiming a compromised system ... 208
Chapter 9: Secure Backup Procedures ... 209
Secure Shell and Secure FTP ... 209
Applicable platforms or hardware ... 209
Symmetric algorithms ... 210
Host keys ... 211
Enabling secure sessions on circuit packs ... 212
Disabling secure sessions on circuit packs ... 213
Enabling secure sessions on Crossfire ... 213
Disabling secure sessions on Crossfire ... 214
Secure updates of Avaya software and firmware ... 215
Enabling or disabling access protocols ... 215
Secure backup procedures for Communication Manager servers ... 216
S8510 and Duplicated Series secure backups ... 216
S8300D Server secure backup procedures ... 218
Viewing backup history ... 221
Schedule Backup ... 222
Adding or changing a scheduled backup ... 222
Add New Schedule field descriptions ... 223
Removing a scheduled backup ... 224
Viewing backup logs ... 225
Backup logs field descriptions ... 225
Viewing and restoring backup data files ... 226
Types of backup files ... 227
Checking backup status ... 227
Chapter 10: Component replacement ... 229
Variable-speed fans ... 229
Replacing variable-speed fans ... 229
Replacing the fan power filter ... 230
Replacing the temperature sensor ... 231
Replacing media modules ... 232
Server circuit packs reseat and replacement ... 232
S8300D Server component maintenance ... 233
G650 component maintenance ... 234
Removing or replacing G650 fan ... 234
Replacing a BIU or rectifier ... 235
Installing BIU or rectifier ... 236
Chapter 11: Packet And Serial Bus Maintenance ... 237
Packet-bus faults isolation and repair ... 237
Remote versus on-site maintenance ... 237
Packet bus ... 238
Packet-Bus faults ... 239
Packet bus connectivity ... 241
Circuit packs that use the packet bus ... 241

Effects of circuit-pack failures on the packet bus ... 242
Packet bus maintenance ... 244
Correcting general fault ... 246
Maintenance/Test circuit pack (TN771D) ... 246
TN771D standalone mode ... 249
Special precaution for the TN771D ... 255
Packet bus fault isolation ... 256
Troubleshooting procedures ... 263
Detecting circuit pack fault ... 263
Removing and reinserting port circuit packs ... 264
PN's control circuit packs removal and reinsertion ... 265
Repairing packet bus faults in simplex control circuit packs ... 265
Configuring high- and critical-reliability systems ... 266
Isolating failures ... 267
G650 Serial Bus fault detection and isolation ... 269
Removing and reinserting port circuit packs one or more at a time ... 271
Serial Bus failure isolation ... 272
Chapter 12: Additional maintenance procedures ... 275
SBS maintenance ... 275
No Media Processor issues ... 275
Signaling group maintenance ... 276
SBS trunk service states ... 276
Trunk member status ... 276
SBS extension status ... 277
Parties involved in an SBS call ... 277
Errors and denial events ... 278
System resets ... 279
Upgrades ... 279
Duplication interactions ... 279
Traffic measurement ... 279
IPSI circuit pack reuse ... 281
Moving from dynamic to static addressing ... 281
Moving from static to dynamic addressing ... 284
Software, firmware, and BIOS update ... 284
DS1 span testing with a loopback jack ... 285
Loopback Jack installation ... 286
Administering loopback jack ... 287
DS1 span tests ... 287
Loopback Jack fault isolation procedures ... 290
Fiber multiplexers testing configurations ... 299
Facility test calls ... 299
Trunk test call ... 300
DS0 loop-around test call ... 302
DTMR test call ... 302
TDM bus time slot test call ... 303
Out-of-service time slot test call ... 305
Placing a call to test the system tone ... 306

Gateway batteries ... 309
Server UPS batteries ... 309
Analog tie trunk back-to-back testing ... 310
Testing using the E&M mode ... 310
Testing using the Simplex mode ... 314
TN760E tie trunk option settings ... 315
Signaling formats for TN760E ... 315
Signaling type summary ... 316
TN464E/F option settings ... 317
TN464E/F option ... 318
Terminating trunk transmission testing ... 319
Power removal and restoration ... 320
Removing and restoring power to multicarrier cabinets ... 320
Removing and restoring power to Gateways ... 321
Removing and restoring power to the mains power source ... 321
Duplicated Series Server power removal and restoration ... 321
Neon voltage (ring ping) ... 324
Adjusting the neon voltage ... 324
Removing power on the G450 and G430 gateways ... 325
Restoring power on the G450 and G430 gateways ... 326
Automatic Transmission Measurement System ... 328
ATMS test ... 329
ATMS reports ... 334
ATMS summary report ... 335
ATMS detail report ... 337
ATMS measurement analysis ... 339
IP telephones troubleshooting ... 340
Telephone does not activate after a power interruption ... 340
Characters do not appear on the display screen ... 341
Display shows an error/informational message ... 341
Unable to get the dial tone ... 341
Echo, noise or static is heard while using a headset ... 342
Telephone does not ring ... 343
Speakerphone does not operate ... 343
Index ... 347

Chapter 1: Overview

This book contains procedures to monitor, test, maintain, and troubleshoot an Avaya Server or Gateway system. Simple and 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, the Avaya business partner's technicians, and the customers should be able to follow detailed procedures for:

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

This book addresses only the issues that can be solved by using:

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

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

Audience

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

- Trained Avaya technicians
- Maintenance technicians visiting the customer site in response to a trouble alarm or a user trouble report
- Maintenance technicians at a remote maintenance facility
- Maintenance technician assigned by the customer

Note:

A technician is expected to have knowledge of telecommunications fundamentals and of the particular Avaya Server and/or Gateway to the extent that the procedures in this book can be performed with little or no assistance.

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.

Observing safety precautions

About this task

Before you attempt repairing any equipment, observe the prescribed safety precautions to avoid unnecessary damage to the equipment and disruption of service. Make the items on the following list a regular part of your safety routine:

Warning:

Failure to comply with these procedures may lead to catastrophic effects on a system hardware and service. Read the following to ensure a complete understanding of these necessary procedures.

Procedure

1. Before touching any component inside a cabinet, use the grounding wrist strap attached to the cabinet frame to avoid sources of static electricity. For more information, see Electrostatic discharge on page 15.
2. When you log on to Avaya Site Administration, alarm notification is normally disabled. For more information, see Suppressing alarm origination on page 16. Log off Avaya Site Administration when you leave the system.
3. Always busyout a server before you turn it off.
4. Do not turn off either a switch node or port carrier to replace a board.
5. Handle fiber-optic cables with care. Bending, piercing, or cutting a cable can sever communications between major subsystems.
6. To disconnect a fiber-optic cable, grasp both the lightwave transceiver and the cable connector.
7. When you finish working on a cabinet, replace and secure every panel and cover to avoid disseminating electromagnetic interference.
8. Before turning off a cabinet or carrier, when the Communication Manager Messaging application enabled (S8300D), first stop the Communication Manager Messaging application to avoid corruption of the application's LDAP database. For instructions on stopping the application, see the Communication Manager Messaging documentation, and in Hot swapping media modules on page 47.

Electrostatic discharge

Poor Electrostatic discharge (ESD) grounding may not cause problems in highly controlled environments. Damage and disruption can happen in less ideal conditions, such as when the air is dry. Following are a few safety measures to avoid system damage or service disruption from ESD:

- You must attach a grounding wrist strap to the cabinet and to your wrist while a circuit pack is inserted or removed.
- You must use a wrist strap while touching any component inside a system's cabinet (including EMERGENCY TRANSFER switches).

- If a wrist strap is unavailable, you must touch the outside panel of the cabinet with one hand before touching any components, and you must keep your other hand grounded throughout the procedure.
- You must handle a circuit pack only by its faceplate, latch, or top and bottom edges. Do not touch board components, leads, or connector pins.
- You must keep circuit packs away from plastic and other synthetic materials, such as polyester clothing. Do not place a circuit pack on a poor conductive surface, such as paper. If available, use an anti-static bag.

Warning:

Never hand a circuit pack to someone who is not using a grounding wrist strap or who is not safely grounded.

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

Procedure

Log in to Communication Manager using the craft login.

- When you log in through a local terminal, the Avaya alarm receiving system does not receive any alarm reports. After logging off, the system automatically resumes alarm origination and reports any unresolved alarms to the alarm receiver.
- When you log in through a 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, unresolved alarms are reported to Avaya alarm receiving system. If you are logged in as craft at two terminals, the log off 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

Documentation

The following table lists the additional documentation related to this document. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Understanding			
03–300468	Avaya Aura® Communication Manager Overview	Describes functionality, features, and deployment scenarios of Avaya Aura® Communication Manager	Sales engineers, implementation engineers, support personnel
555-245-207	*Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207	Provides information about hardware that Avaya Aura® Communication Manager supports	Sales engineers, implementation engineers, support personnel
Installing			
03-601508	Installing and Operating a 120A Channel Service Unit with Avaya Aura® Communication Manager	Contains procedures for installing and operating a 120A channel service unit (CSU) on a media gateway.	Sales engineers, implementation engineers, support personnel
03-602055	Installation and Upgrades from the G450 Branch Gateway	Contains procedures for installing and upgrading the G450 Branch Gateway	Sales engineers, implementation engineers, support personnel
03-603233	Installation and Upgrades from theG450 Branch Gateway	Contains procedures for installing and upgrading the G450 Branch Gateway	Sales engineers, implementation engineers,

Document number	Title	Description	Audience
			support personnel
03-602056	CLI Reference G450 Branch Gateway	Describes the commands used to configure and manage the G450 Media Gateway after it is already installed	Sales engineers, implementation engineers, support personnel
03–603234	CLI Reference G430 Branch Gateway	Describes the commands used to configure and manage the G430 Branch Gateway after it is already installed	Sales engineers, implementation engineers, support personnel
	Avaya P333T User's Guide	Contains information about application, installation and set up of Avaya P333T stackable switches	Sales engineers, implementation engineers, support personnel
03-603633	*Avaya Aura® Communication Manager Survivable Options*, 03-603633	Contains information about Survivable core server installation, conversion, and troubleshooting.	Sales engineers, implementation engineers, support personnel
03-300685	Installing the G450 Media Gateway	Contains procedures to install a new G450 Media Gateway connect it to the customer's network, and test the complete configuration.	Sales engineers, implementation engineers, support personnel
555-233-775	4606 IP Telephone User's Guide	Describes the 4606 IP Telephone's operation and functionality	Sales engineers, implementation engineers, support personnel
555-233-777	4612 IP Telephone User's Guide	Describes the 4612 IP Telephone User's Guide	Sales engineers, implementation engineers, support personnel

Document number	Title	Description	Audience
03-300538	Job Aids for Field Replacement Units for the S8300D Server with G450 Branch Gateway or G430 Branch Gateway	Describes the procedures to replace an installed S8300D Server or the S8300D hard drive.	Sales engineers, implementation engineers, support personnel
555-245-702	The Avaya RSA Users' Guide	Provides procedures to administer your Remote Supervisor Adapter (RSA) on the Avaya S8500 Media Server	Sales engineers, implementation engineers, support personnel
03-603560	Upgrading Avaya Aura® Communication Manager	Provides the process and procedures for upgrading Avaya Aura® Communication Manager to Release 6.0.1. Communication Manager	Sales engineers, implementation engineers, support personnel
03–602884	Converting Avaya Servers and Branch Gateways	Describes procedures for conversions of Avaya telecommunication products that use Avaya Aura® Communication Manager	Sales engineers, implementation engineers, support personnel
Administration			
03-300509	Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager	Sales engineers, implementation engineers, support personnel

Chapter 2: Maintenance strategy

The maintenance subsystem is the part of a system that is responsible for initializing and maintaining the system. This subsystem continuously monitors the condition of the system 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 overall functions of the system. For detailed descriptions of components and subsystems, refer to related topics in the Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gatewayand Servers, *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

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. An MO 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

Note:

Each MO is referred to by an uppercase, 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 physical location of an MO 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 for Avaya Aura® Communication Manager, Branch Gatewayand Servers, *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430includes 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)
- The DS1 Tie Trunk circuit pack (TIE-DS1)
- The 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)
- Duplicated servers 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 the environmental sensors of a cabinet (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 for Avaya Aura® Communication Manager, Branch Gatewayand Servers, *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 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)

- 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	60
MED-GTWY	120
NR-CONN	5
POWER	60
TDM-BUS	10
TONE-PT	10

Demand testing

Any other kind of maintenance testing apart from periodic, scheduled, fixed-interval testing is referred to as demand tests.

- Includes periodic tests. Other tests are required only when trouble occurs.
- Can be run by the system when the system detects a need or can be run by maintenance personnel in troubleshooting 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, software performs a periodic test or a scheduled test on occurrence of an error.

Note:

On demand, by using the maintenance commands described in Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431) and the maintenance objects in Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gatewayand Servers, *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430, the technician can run periodic and scheduled tests.

When an error is detected, the maintenance software records 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. The alarm and error logs are displayed locally on the management terminal. Depending on the alarm's effect on system operation, an alarm is classified as MAJOR, MINOR, or WARNING. 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.

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

Communication Manager sends the alarms to Secure Access Link (SAL) Gateway. SAL Gateway sends the major or minor alarms to Avaya Services Ticketing System.

For more information about Virtual SAL Gateway, Stand-alone SAL Gateway, and Configuring SAL Gateway, see Administering Avaya Aura® System Platform.

If multiple alarms are reported against a given MO, the level of the alarm changes. For example,

- If an active error causes a minor alarm, and another active error causes a major alarm, the alarm log shows two major alarms.
- If the minor alarm is resolved first, the error is marked as alarmed until the major alarm is resolved, and alarm log shows two major alarms.
- If 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.

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.

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

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.

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 Remote Max Alarms.

Alarm reporting options screens

The Alarm Reporting Options screens display many ways to configure Communication Manager for detailed maintenance information.

```
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 1: Set options form, page 1

```
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
                               H.248 Media Gateway Alarms: m      w
```

Figure 2: Set options form, page 2

Trunk group alarm options

You can use the pages 3 to 22 of the Alarm Reporting Options to group trunk groups and to administer a collective alarm reporting strategy. For example, the Trunk group alarm options page on page 27 shows the first 100 trunk groups by number.

```
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
```

Figure 3: Trunk group alarm options page

In this screen 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 Set options form on page 26). 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 Set options form on page 26). 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 Set options form on page 26). 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 Set options form on page 26). 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-powered 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 Expansion Port Network (EPN), all the services to that port network are dropped, and the EPN must be reset when power is restored.
- If the EPN contains a switch node carrier, all the services to port networks connected to that switch node are dropped.

Single-carrier cabinets that are used as EPNs have no battery backup. If power is interrupted for more than 0.25 seconds, all the services are 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

The 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. The nominal power holdover feature is optional on cabinets supplied by a UPS and is 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 administration of the cabinet. See the table on page 29 for duration times.

Using nominal power holdover controlled by software, the system sustains 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 or the charger must be replaced.

Note:

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. You can run **test maintenance UU** (where **UU** is the cabinet number) to verify whether your cabinet administration is correct. If it is incorrectly administered to all-carriers, a warning alarm is issued and you must re-administer the cabinet to a-carrier-only.

Table 1: Nominal power holdover

Cabinet administration	Control carrier holdover duration	Entire cabinet holdover duration
a-carrier-only	10 minutes	15 seconds
all-carriers	2 minutes	2 minutes

Power interruption effects

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. In such a situation certain maintenance objects such as, external DS1 timing reports a major alarm. When power is restored, the AC-POWER alarm is resolved.

External alarm leads

Each cabinet provides two leads: one for major and one for 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 UPS or battery reserves powering the switch. They are also commonly used to monitor adjuncts such as, Communication Manager Messaging.

Communication Manager Messaging

Stopping the Communication Manager Messaging application manually

About this task

An amber caution sticker on the power unit of the system notifies technicians to shut down the Communication Manager Messaging application prior to stopping the application. Use this procedure to manually shut down the Communication Manager Messaging application.

Procedure

Using a pointed object such as a paper clip or pen (do not use a pencil), press and release the **Boot/Shutdown** button located at the top right portion of the front panel.

Note:

The Communication Manager Messaging application takes about five minutes to shut down. The heartbeat indication on the display continues to flash.

Starting the Communication Manager Messaging application manually

About this task

Use this procedure to manually start the Communication Manager Messaging application.

Procedure

1. Using a pointed object such as a paper clip or a pen (do not use a pencil), press and hold the **Boot/Shutdown** button until the display indicates the message BTEST steady on.
2. Release the **Boot/Shutdown** button.

   The Communication Manager Messaging application takes approximately five minutes to start. The display has the following sequence of steady-on messages:

   - OSINIT
   - OS
   - AINIT
   - ADX

   The Communication Manager Messaging application is now started. When the system is in the active state, the display indicates `ADX`, and the red LED is off.
3. When turning on, the Communication Manager Messaging application automatically reboots. This sequence may show an MD or MJ ADX alarm in the

display until the application has turned on. When the system has completed its booting up sequence, the display reads ADX.

Connecting S8300D Server to a Media Gateway processor when IP forwarding is enabled

About this task

Use this procedure to establish a SSH connection between S8300D Server and a Media Gateway processor on the same backplane LAN when IP forwarding is enabled.

Procedure

1. Run ping or traceroute 169.254.1.11.
2. Use SSH <BGW login>@169.254.1.11 to connect to the gateway. <BGW login> should be:
    - a customer login that was established for the Business Partner
    - an ASG protected login that Avaya services may use, or
    - a customer using their own login.

Connecting S8300D Server to a Media Gateway processor when IP forwarding is disabled

About this task

Use this procedure to establish a SSH connection between S8300D Server and a Media Gateway processor on the same backplane LAN when IP forwarding is disabled.

Procedure

1. Run ping or traceroute 169.254.1.11.
2. Obtain the admin password from the customer.
3. Log in to the dom0 shell using admin credentials.
4. Run **`service_port_access disable or ip_forwarding enable`** command.
5. Log out of dom0.
6. Use SSH <BGW login>@169.254.1.11 to connect to the gateway. <BGW login> should be:
    - a customer login that was established for the Business Partner,

- an ASG protected login that Avaya services may use, or
- a customer using their own login.

Protocols

This section describes the protocols handled by the system and the points where these protocols change. The figure on page 33 is a pictorial guide through intra-port and inter-port data transmission state changes. The pictorial guide illustrates the flow of data from DTE equipment, through DCE equipment, 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 the figure on page 33 is the treatment of D-channels in ISDN-PRI and ISDN-BRI transmissions. PRI and BRI D-channels transport information elements contain call-signaling and caller information. These elements conform to ISDN level-3 protocol. In case of BRI, the elements are created by the terminal or data module. In case of PRI, the elements are created by the system. The system inserts the elements 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 Open Systems Interconnection model on page 32.

Open Systems Interconnection model

The Open Systems Interconnection (OSI) model for data communications contains seven layers, each with a specific function. In the OSI model, data communication uses only 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 the figure on page 33 as user-defined, with no state changes until the transmission stream reaches its destination.

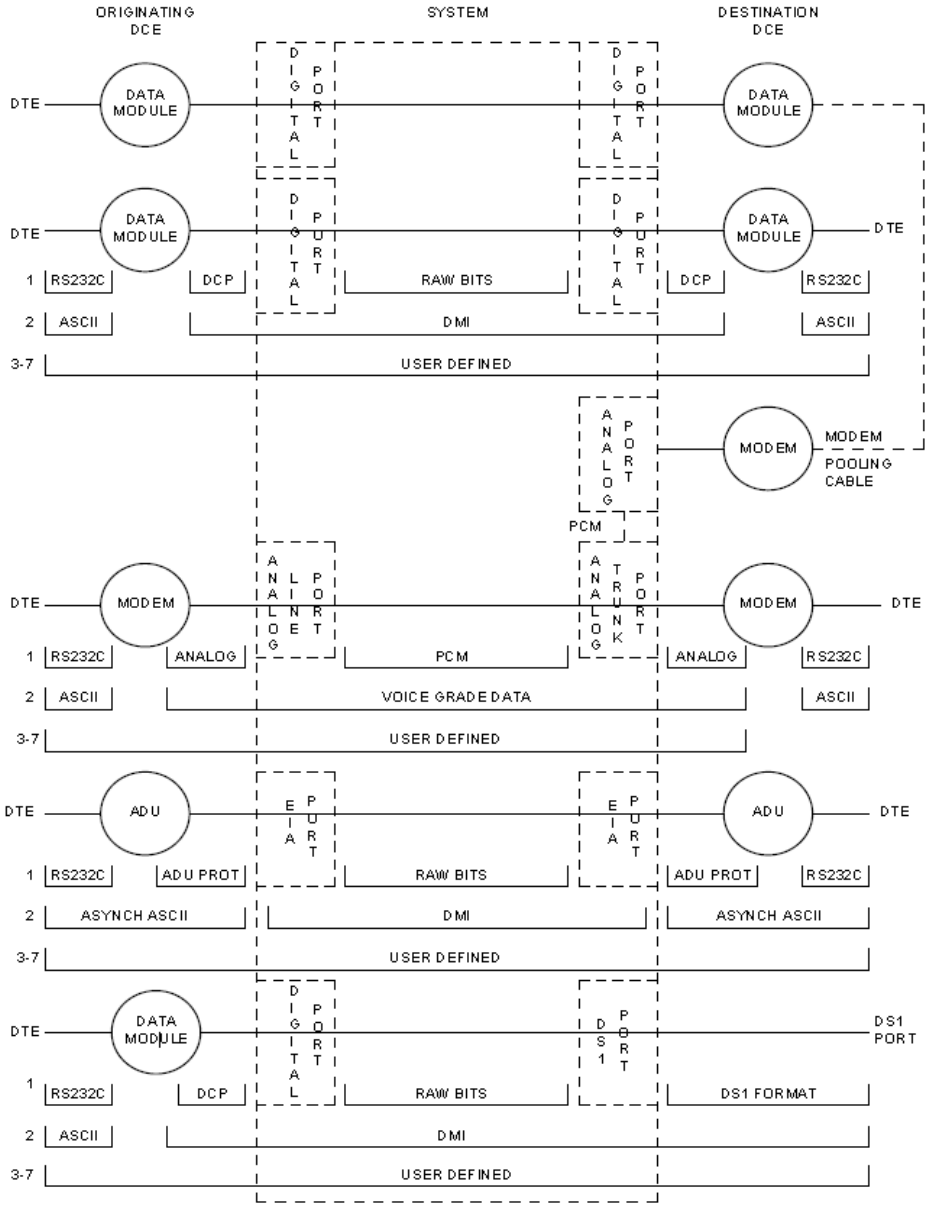


Figure 4: Intra-port and Inter-port data transmission states

Protocol usage

This section describes a list of the protocols that are used when data is transmitted to and through the system. The list is organized by protocol layers. For more information, see the figure on page 33.

Layer-1 protocols

Layer-1 protocols are used between the terminal or the host DTE and the DCE. The protocols are used between the DCE equipment and the system port, and 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 24-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 occurs in one of the 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 is digitized by an analog-to-digital coder/decoder (CODEC) at the incoming port.

Layer-2 protocols

- 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 and used for analog transmission.

Protocol states

The following table summarizes the protocols used at various points in the data transmission stream. See also the figure on page 33.

Pulse Code Modulated is known as PCM and Digital Multiplexed Interface is known as DMI.

Table 2: Protocol states for data communication

Transmission type	Incoming DTE to DCE	OSI layer	Protocols DTE to DCE	DCE to system port	Inside system
Analog	Modem	1	RS-232, RS-449, or V.35	analog	PCM

Transmission type	Incoming DTE to DCE	OSI layer	Protocols DTE to DCE	DCE to system port	Inside system
		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
Digital	Data Module	1	RS-232, RS-449, or V.35	DCP or BRI	Raw bits
		2	8-bit code	DMI	DMI
	Digital Signal Level 1 (DS1)	1	Any	DS1	PCM or raw bits
		2	8-bit code	DMI or voice-grade data	DMI or voice-grade data

The physical-layer protocol and the 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 the table on page 36 and the table on page 36.

Table 3: 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 4: 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

The figure on page 33 implies the following connectivity rules:

- Only the DS1 port and the analog trunk port are trunking facilities (every other port is a line port). For communication over these facilities, the destination DCE equipment can

be a hemisphere away from the system, and the signal can traverse any number of intervening switching systems before reaching the destination equipment.

- Data originating at any type of digital device, whether DCP or BRI, can exit the system at any type of digital port — BRI, digital-line, PRI, DS1, and others; as long as the call destination is equipped with a data module using the same DMI mode used at the call origin. This is because once the data enters the system through a digital port, its representation is uniform (raw bits at Layer 1, and DMI at level 2), regardless of where it originated.
- Although data entering the system through an EIA port has not been processed through a data module, the port itself has a built-in data module. Inside the system, port data is identical to digital line data. Data entering the system at a DCP line port can exit at an EIA port. Conversely, data entering the system at an EIA port can exit at any DCP line port. The destination data module must be set for Mode-2 DMI communication.
- Voice-grade data can be carried over a DS1 facility as long as the destination equipment is a modem compatible with the originating modem.
- If a mismatch exists between the types of signals used by the endpoints in a connection (for example, the equipment at one end is an analog modem, and the equipment at the other end is a digital data module), a modem-pool member must be inserted in the circuit. When the endpoints are on different switches, it is recommended that the modem-pool member be put on the origination or destination system. A modem-pool member is always inserted automatically for calls to off-premises sites via analog or voice-grade trunking. For internal calls, however, the systems are capable of automatically inserting a modem-pool member.
- Data cannot be carried over analog facilities unless inside the system it is represented as a PCM-encoded analog signal. To do this for data originating at a digital terminal, the signal enters the system at a digital port and exits the system at a digital port. The signal then reenters the system through a modem-pool connection (data-module to modem to analog-port) and exits the system again at an analog port.
- Although DS1 is commonly called a trunk speed, here it names the protocol used at Layer 1 for digital trunks. Some trunks use different signaling methods but use DS1 protocol at Layer 1 (for example, PRI and 24-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 cannot terminate 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 can 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 following are the possible outcomes:

- 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 call can be transferred, and the other system is queried for disconnect supervision.
- 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.
- 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.

- If a station conferences every party, the conference can occur 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.
- 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

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

Table 5: 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

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

Table 6: 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

The table on page 40 lists the insertion loss in the system for port-to-port, analog, or digital connections in the United States.

Table 7: 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

The table on page 40 shows the overload and cross-talk.

Table 8: Overload and crosstalk

Overload level	+3 dBm0
Crosstalk loss	>70 dB

Intermodulation distortion

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

Table 9: Intermodulation distortion

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

Quantization distortion loss

The table on page 41 lists the quantization distortion loss in the system for analog port to analog port.

Table 10: 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

The table lists the quantization distortion loss in the system for analog port-to-digital port and digital port-to-analog port.

Table 11: Quantization distortion loss

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

Note:

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 the table on page 41.

Table 12: ERL and SFRL performances by connection type

Type of connection	ERL and SFRL performance
Station-to-station	ERL should meet or exceed 18 dBSFRL should meet or exceed 12 dB
Station to 4-wire trunk connection	ERL should meet or exceed 24 dBSFRL should meet or exceed 14 dB

Type of connection	ERL and SFRL performance
Station to 2-wire trunk connection	ERL should meet or exceed 18 dBSFRL should meet or exceed 12 dB
4-wire to 4-wire trunk connection	ERL should meet or exceed 27 dBSFRL should meet or exceed 20 dB

Peak noise level

The table on page 42 lists the peak noise level.

Table 13: Peak noise level

Type of connection	Peak noise level (dBrnC)
Analog to analog	20
Analog to digital	19
Digital to analog	13
Note: Decibels above reference noise with C-filter.	

Echo path delay

The table on page 42 lists the echo path delay.

Table 14: Echo path delay

From	To	Delay (ms)
Analog port	Analog port	≤ 3
Digital interface port	Digital interface port	≤ 2

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 for 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.

Facility Interface Codes list

The table on page 43 through the table on page 44 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 15: 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 16: 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 andRJ48 M

Table 17: 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

The Multimedia Interface (MMI) 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 the BRI interface of a personal computer.

Maintenance of G430 Branch Gateway and G450 Branch Gateway and servers

You can use the following applications to manage G430 Branch Gateway and G450 Branch Gateway:

- The Avaya G450 Branch Gateway and G430 Branch Gateway Command Line Interface (CLI)
- System Management Interface
- Avaya QoS Manager
- Avaya G450 Branch Gateway and G430 Branch Gateway Manager

You can access G430 Branch Gateway and G450 Branch Gateway and S8300D in the following ways:

- Web server access to the gateway or server IP address (accesses web page with online help)

  Note:

  Since G430 Branch Gateway and G450 Branch Gateway also function as WAN routers, they can have more than one IP interface.

- .Avaya Site Administration
- Remote access through an external serial analog modem connected to G430 Branch Gateway and G450 Branch Gateway Console port
- A console device connected to the Console port on G430 Branch Gateway and G450 Branch Gateway front panel.

Maintenance Web Interface

The Maintenance Web Interface is a browser-based web administration interface used to administer the G450 Branch Gateway and G430 Branch Gateway on the corporate local area network (LAN). This administration interface is an efficient way to configure the G450 Branch Gateway and G430 Branch Gateway, the Media Server, and media modules. In addition to initial administration, you can do the following:

- check server status
- perform software and firmware upgrades
- back up and restore data files
- enable the USB and Console ports for use with a modem, thereby enabling remote upgrades

The Maintenance Web Interface complements the other server administration tools, such as the System Access Terminal (SAT) emulation program and the Avaya Site Administration telephony application. The Maintenance Web Interface focuses on the setup and maintenance of the S8300D Server with the G450 Branch Gateway and G430 Branch Gateway.

Avaya G450 Branch Gateway and G430 Branch Gateway CLI

Avaya G450 Branch Gateway and G430 Branch Gateway Command Line Interface (CLI) provides access to configurable and read-only data on all the G450 Branch Gatewayand G430 Branch Gateway subsystems as well as running tests and displaying results. As a minimum, the CLI supports all functionality the Device Manager provides. It provides access to the status, parameters, and testing of media modules, IP Entity Configuration, TFTP/FTP servers, and DSP or VoIP resources. For a detailed description of the CLI commands, see CLI Reference Avaya Branch Gateway G450 Branch Gateway, 03-602056 and CLI Reference Avaya Branch Gateway G430 Branch Gateway, 03-603234

G430 Branch Gateway and G430 Branch Gateway maintenance strategy with S8300D

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 need to move G450 Branch Gateway and G430 Branch Gateway toward a data networking paradigm. This leads to a dual strategy in which some of the subsystems of G450 Branch Gateway and G430 Branch Gateway are maintained and controlled by a server running Communication Manager, while others are covered by maintenance software residing on G450 Branch Gateway and G430 Branch Gateway. The latter subsystems are not monitored directly by a server.

The table on page 46 shows the three main maintenance arenas associated with S8300D Server with G450 Branch Gateway and G430 Branch Gateway gateways:

Table 18: Avaya Servers and Gateways maintenance arenas

Arena	Detail
Web Interface	Web-based access to the S8300D or Duplicated 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
G450 Branch Gateway and G430 Branch Gateway CLI commands	Unique to the G450 Branch Gateway and G430 Branch Gateway platform. Used for administration, maintenance, and status functions on G450 Branch Gateway and G430 Branch Gateway. For more information on to access the Layer 2 Switching Processor CLI for Layer 2 Switching

Arena	Detail
	Processor-related CLI commands, see CLI Reference Avaya Branch Gateway G450, 03-602056 and CLI Reference Avaya Branch Gateway G430, 03-603234.

Hot swapping media modules

Gateway Media Module maintenance is controlled by Communication Manager and is very similar to that for corresponding TN circuit packs. Field replacement of some Media Modules can be performed without removing power to the gateway, also known as hot swapping. However, G450 Branch Gateway and G430 Branch Gateway will reset for other modules.

Warning:

Hot swapping is not recommended for data modules because inserting the board resets G450 Branch Gateway and G430 Branch Gateway, and any translation and other data that are in the running configuration but have not been saved to the startup configuration are lost.

Caution:

The Avaya Expansion Modules and Cascade Modules are not hot-swappable. They are service-disrupting and can reset the entire G450 Branch Gateway and G430 Branch Gateway upon insertion or removal. Turn off the system, including shutting down S8300D Server hard drive, if present, prior to any insertion or removal of Avaya Expansion and Cascade modules.

The following Avaya Media Modules are hot-swappable:

- DCP Media Module (MM712/MM717)
- Analog Trunk/Telephone Port Media Module (MM711/MM714/MM716)
- T1/E1 Media Module (MM710)
- BRI Media Module (MM720/MM721/MM722)

For procedures on adding, removing, or replacing Media Modules, refer to S8300D component maintenance on page 233.

Caution:

S8300D is not hot swappable. S8300D Server can reset G450 Branch Gateway and G430 Branch Gateway, which are registered, upon insertion or removal. When removing the S8300D, you can initiate a shutdown process by first keeping the button, which is located next to the fourth GREEN Ok-to-Remove LED (specific to S8300D), pressed (for 2 seconds). This LED will first blink and then go steady. Once steady, the GREEN LED indicates that the disk drive has been shut down properly and is ready to be removed. If you remove

S8300D before the disk is shut down, you may corrupt important data. See S8300D component maintenance on page 233.

Note:

This server can be a primary server for a network of IP endpoints and G450 Branch Gateway and G430 Branch Gateway, or it can be configured as a Survivable Remote Server, to become active only if connectivity to the primary server is lost. Most of the material in this book applies to the S8300D Server configuration; only a few parts apply to the Survivable Remote Server configuration.

G450 and G430 server-controlled maintenance

Communication Manager equivalent elements

Many of the Avaya Media Modules and gateway subsystems are based on existing Communication Manager circuit packs or systems as listed in the table on page 48. Media Module component functions are maintained equivalently to their Communication Manager counterparts.

Note:

This information is included for environments where the gateway with an Avaya Server is integrated into larger architectures running Communication Manager.

Table 19: Communication Manager equivalent elements of

Gateway component	Communication Managerequivalent
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
S8300D	Duplicated server or other DEFINITY ECS
Communication Manager Messaging S8300D	IA770 Intuity Audix messaging
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 markedly differ from their Communication Manager counterparts, which along with the G450 Branch Gateway and G430 Branch Gateway changes how many operations are conducted.

Capacity constraints and feature limitations

Although Media Modules and other G450 Branch Gateway and G430 Branch Gateway components have functionality similar to Communication Manager 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 Communication Manager server version.

These differences, as well as the fact that G450 Branch Gateway and G430 Branch Gateway have control over the TDM bus, the tone/clock generator, and the tone detectors means that a 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 G450 Branch Gateway and G430 Branch Gateway.

Media module tests

The the table on page 49 list the permitted and invalid tests for the Media Modules. As shown in this table, the board and port tests are based on existing tests that run on the equivalent 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 Servers.

Note:

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

Table 20: Media module tests

Media Module	Maintenance Object	Test	Executed for Media Module
Analog Media Module (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

Media Module	Maintenance Object	Test	Executed for Media Module
		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
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

Media Module	Maintenance Object	Test	Executed for Media Module
		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
BRI Trunk Media Module (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

Media Module	Maintenance Object	Test	Executed for Media Module
		Signaling Link State Check Test (#1251)	Yes
DCP Media Module (TN2224)	Board (MG-DCP) (DEF DIG-BD)	NPE Audit Test (#50)	Abort
		Control Channel Loop Test (#52)	Yes
		SAKI Sanity Test (#53)	Yes
	Digital Line (DIG-LINE)	Digital Line NPE Crosstalk Test (#9)	Abort
		Digital Line Electronic Power Feed Test (#11)	Yes
		Voice and Control Channel Local Looparound Test (#13)	Abort
		DIG-LINE Station Lamp Updates (#16)	Yes
		Station Audits Test (#17)	Yes
		Digital Terminal Remote Loop Around Test (#1201)	Abort
T1/E1 Media Module (DEF TN464F)	Board (MG-DS1) (DEF UDS1-BD)	NPE Correction Audit Test (#50)	Abort
		Control Channel Loop Test (#52)	Yes
		Loss of Signal Alarm Inquiry Test (#138)	Yes
		Blue Alarm Inquiry Test (#139)	Yes
		Red Alarm Inquiry Test (#140)	Yes
		Yellow Alarm Inquiry Test (#141)	Yes
		Major Alarm Inquiry Test (#142)	Yes
		Minor Alarm Inquiry Test (#143)	Yes
		Slip Alarm Inquiry Test (#144)	Yes
		Misframe Alarm Inquiry Test (#145)	Yes
		Translation Update Test (#146)	Yes
		ICSU Status LEDs Test (#1227)	No
		Echo Cancellation Test (#1420)	Yes
		SAKI Sanity Test (#53)	Yes
		Internal Loop Around Test (#135)	Abort

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

Media Module	Maintenance Object	Test	Executed for Media Module
Voice Announcements (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

G450 Branch Gateway and G430 Branch Gateway testing limitations

G450 Branch Gateway and G430 Branch Gateway subsystems that are under the control of S8300D and Duplicated 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 G450 Branch Gateway and G430 Branch Gateway

Table 21: Tests not executed on G450 Branch Gateway and G430 Branch Gateway

Test	Notes
NPE_AUDIT	This test is really an audit that sends network update messages to various ports on a board. Since the server does not handle network connections for the gateway, 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 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 gateway.
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. Server does not handle network connections, so this test is not run.
ICSU_LEDS	Checks the Integrated Channel Service Unit LEDs, which do not exist on the DS1 Media Module.
DIAL_TONE_TS	Detects dial tone.
TRK_AUTO_GRD	This test is for the Australian version of the CO board, TN438.
TRK_PPM_TEST	Factory only test for certain CO trunks; requires a pulse generator.
TRK_HYB_TS	Tests the loop around capabilities of a port's codec and hybrid circuits.
ONS_HYB_TS	Tests the loop around capability on the codec circuit.
BRI_EPF	Electronic power feed test; not valid for TN2185.
L1_INQ	This function actually encompasses several tests.
SSP_TDMLOOP	This is for the messaging angel, but the server is unaware of the TDM bus.

Test	Notes
PRI_TSTCALL	Requires the use of either a data channel or a maintenance test board, neither of which are present.
TDMLP_BRI	The server cannot use the TDM bus.
PPP_TDMLOOP	The server cannot use the TDM bus.

Tone detector tests not executed on G450 Branch Gateway and G430 Branch Gateway

Table 22: Tone detector tests not executed on G450 Branch Gateway and G430 Branch Gateway

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

Tone generator tests not executed on G450 Branch Gateway and G430 Branch Gateway

Table 23: Tone generator tests not executed on G450 Branch Gateway and G430 Branch Gateway

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

TDM bus tests not executed on G450 Branch Gateway and G430 Branch Gateway

Table 24: TDM bus tests not executed on G430 Branch Gateway and G450 Branch Gateway

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

Maintenance features for G450 Branch Gateway and G430 Branch Gateway

Table 25: Maintenance features for G450 Branch Gateway and G430 Branch Gateway

Supported feature	Controller Duplicated Servers/ S8300D	Notes
Attendant Console alarm LED and alarm report acknowledgement LED	Yes	Status of G450 Branch Gateway and G430 Branch Gateway 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

Supported feature	Controller Duplicated Servers/ S8300D	Notes
		• 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 G450 Branch Gateway and G430 Branch Gateway so DS1 sync is controlled by G450 Branch Gateway and G430 Branch Gateway.
Enable/Disable Media Module tests	Yes	
Enable/Suspend alarm origination	No	Not supported by Duplicated Server platform.
Environment tests and alarms for S8300D		Not available for S8300D in R1.
ISDN loop around connection	Yes	
ISDN test call	No	Not available for ISDN trunks terminating on a DS1 Media Module.
LED tests	Partial	Works with Media Module LEDs but not with G430 Branch Gateway and G450 Branch Gateway 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 G430 Branch Gateway and G450 Branch Gateway, so this does not apply to G450 Branch Gateway and G430 Branch Gateway with S8300D Server. A new MO is added for the status and alarming of H.248 links.
System tone test call for G430 Branch Gateway and G450 Branch Gateway	No	Requires changes to the call processing software in S8300D and the G450 Branch Gateway and G430 Branch Gateway.
TDM Time Slot test call	No	

Supported feature	Controller Duplicated Servers/ S8300D	Notes
Terminating Trunk Transmission test	No	
Test MO command	Yes	Support syntax of Media Module location
Test S8300D hardware	Limited	
Test of G450 Branch Gateway and G430 Branch Gateway resources: Archangel Network Control Element Packet Interface TDM clock Tone generator Tone detectors	No	Provided by G450 Branch Gateway and G430 Branch Gateway. G450 Branch Gateway and G430 Branch Gateway architecture specifies these resources as G450 Branch Gateway and G430 Branch Gateway resources, not S8300D resources.
Tests of Media Modules	Partial	Limited by the tests available in R1.
Touch Tone Receiver facility test call	No	TTRs in G450 Branch Gateway and G430 Branch Gateway are not available outside the gateway.
Touch Tone Receiver level	No	TTRs in G450 Branch Gateway and G430 Branch Gateway are not available outside the gateway.
Trunk facility test call	Yes	
Write Physical Angel command	No	
System synchronization	No	

Chapter 3: Server initialization and network recovery

Duplicated server initialization

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

- VSP: After the server is powered on, Virtual System Platform (VSP) boots the system and performs diagnostic tests on the hardware such as the processor, memory, disks. After VSP completes the hardware tests, control is then passed to the Linux loader (GRUB).
- GRUB: Grand Unified Bootloader (GRUB) is a Linux loader that reads the Linux kernel from the boot disk and transfers control to it. Basic input/output system (BIOS) reads phase 1 of GRUB in to memory. When Phase 1 begins executing, it reads in the rest of the GRUB program including the location of the Linux kernel. GRUB reads the Linux kernel, uncompresses it, and transfers control to the kernel.
- Linux Kernel: The Linux kernel initializes the Pentium processor registers and its own data structures, determines the amount of available memory, and initializes the various compiled-in device drivers. When finished, the Linux kernel creates the first process, known as init.
- 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.
- 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. 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.

- Hardware-Sanity: The Watchdog periodically tells the hardware-sanity device how long to wait for before rebooting the system. If the Hardware-Sanity driver does not receive an update within that interval, the HW Watchdog's timer resets the processor.
- Arbiter: The Arbiter decides whether the server goes active or standby.

Active server initialization

The active server initialization is executed on the server or active server (duplicated).

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, such as 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 initialization

On the standby server, the Communication Manager freezes many processes, 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

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

- IPSI-connected port networks (S8510 | Duplicated servers only)
- IP trunks (signaling groups: (S8510 | Duplicated servers only)
- All gateways

Note:

The Avaya S8300D Server does not support port networks. And, while the S8300D can have IP trunks, it does not monitor their status. 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.

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

- Survivable Core Server: Applies to the connections between the Survivable Core Server and those port networks, gateways, and signaling groups that the Survivable Core Server is actively controlling.
- Survivable Remote Server: Applies to S8300D Server, S8510 (through the Processor Ethernet interface), S8800, HP DL360 G7, or Dell R610 Servers functioning as a Survivable Remote Server and the gateway connections that the Survivable Remote Server is actively controlling.

Hardware and software requirements

Automatic trace-route feature requires:

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

Note:

In a standard installation the Automatic trace-route feature is ON by default.

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 gateway. A link to a 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 S8300D) 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.

Administration

Administering automatic trace-route through SMI

About this task

You can administer automatic trace-route from System Management Interface (SMI). Use this procedure to administer the Automatic trace-route feature through SMI.

Procedure

1. Log in to the System Management Interface.
2. Select **Diagnostics** > **Traceroute**.

   The system displays the Traceroute page.
3. In the **Host name or IP address** field, enter either the host name or the IP address.
4. Select the Print address numerically option to print the hop addresses numerically rather than by symbolic name and number.

   If you do not select the Print address numerically option, the system looks up symbolic names for the host addresses. To do so, the system uses the domain name server, which translates the IP address to a symbolic name. If the domain name server is unavailable, the traceroute command will be unsuccessful.
5. Select the Bypass routing tables and send directly to host option to run the traceroute to a local host through an interface that has no route through it.

   The Bypass routing tables and send directly to host option runs the traceroute to a local host on an attached network. If the host is not on a network that is directly attached, the traceroute will be unsuccessful and you will receive an error message.
6. Select the Use alternate IPv4 address as the source address option to specify an alternate IP address as the source address.

   Use the Use alternate IPv4 address as the source address option to force the source address to be something other than the IP address of the interface from which the probe packet was sent.
7. Click **Execute Traceroute**.

Administering automatic trace-route through SAT

About this task

With proper permissions you can turn the automatic trace-route feature on and off from the system access terminal (SAT). Use this procedure to administer the Automatic trace-route feature through SAT.

Procedure

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

   The system displays the IP-Options System Parameters page.

```
change system-parameters ip-options
                                                          Page   1 of   4
                          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
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
   Server IPV4 Address:                 RTCP Report Period(secs): 5
              IPV4 Server Port: 5005
   Server IPV6 Address:
              IPV6 Server Port: 5005
AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                      H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                   Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5         Primary Search Time (sec): 75
                                Periodic Registration Timer (min): 20
                              Short/Prefixed Registration Allowed? n
```

   Figure 5: IP-Options System Parameters form

2. To enable the automatic trace-route command, set the **AUTOMATIC TRACE ROUTE** field to ON and **Link Failure** field to y.
3. To disable the automatic trace-route command, set the **AUTOMATIC TRACE ROUTE** field to ON and **Link Failure** field 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).

4. Press Enterto submit the form.

Command results

The logged results of the trace-route command can help you determine network outages that cause link failures.

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. For more information about the trace-route command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431. See Conditions and interactions on page 71 for command precedence information.

Viewing results through SMI

About this task

Use this procedure to view the results of the **`trace-route`** command in the Maintenance Web Pages.

Procedure

1. Log in to the System Management Interface (SMI).
2. From the left side select **Diagnostics** > **System Logs**.
   The System Logs page displays.
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 Web interface log entries interpretation on page 68 section describes the various log entry types.

Viewing results through SAT

About this task

Use this procedure to view the results of the trace-route command in the Linux log file.

Procedure

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 gateway logs, respectively.

2. The Web interface log entries interpretation on page 68 section describes the entries associated with the trace-route command.

Web interface log entries interpretation

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 system displays the following information 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), gateway number (for 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

Note:

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

Mediagateway link failures

In addition to the generic information, the log shows an example of a 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 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) shuts down abnormally; 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 abnormal shut downs are not logged in the IP events log; the Linux OS logs should indicate that the OS restarted.

  - Duplicated servers 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. 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.

- S8300D and S8510 Server only: RAM disk configuration supports server reliability by partially surviving a disk failure. 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 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.

The figure on page 73 depicts the recovery timers that work together to reroute network connections.

Recovery timers and interactions

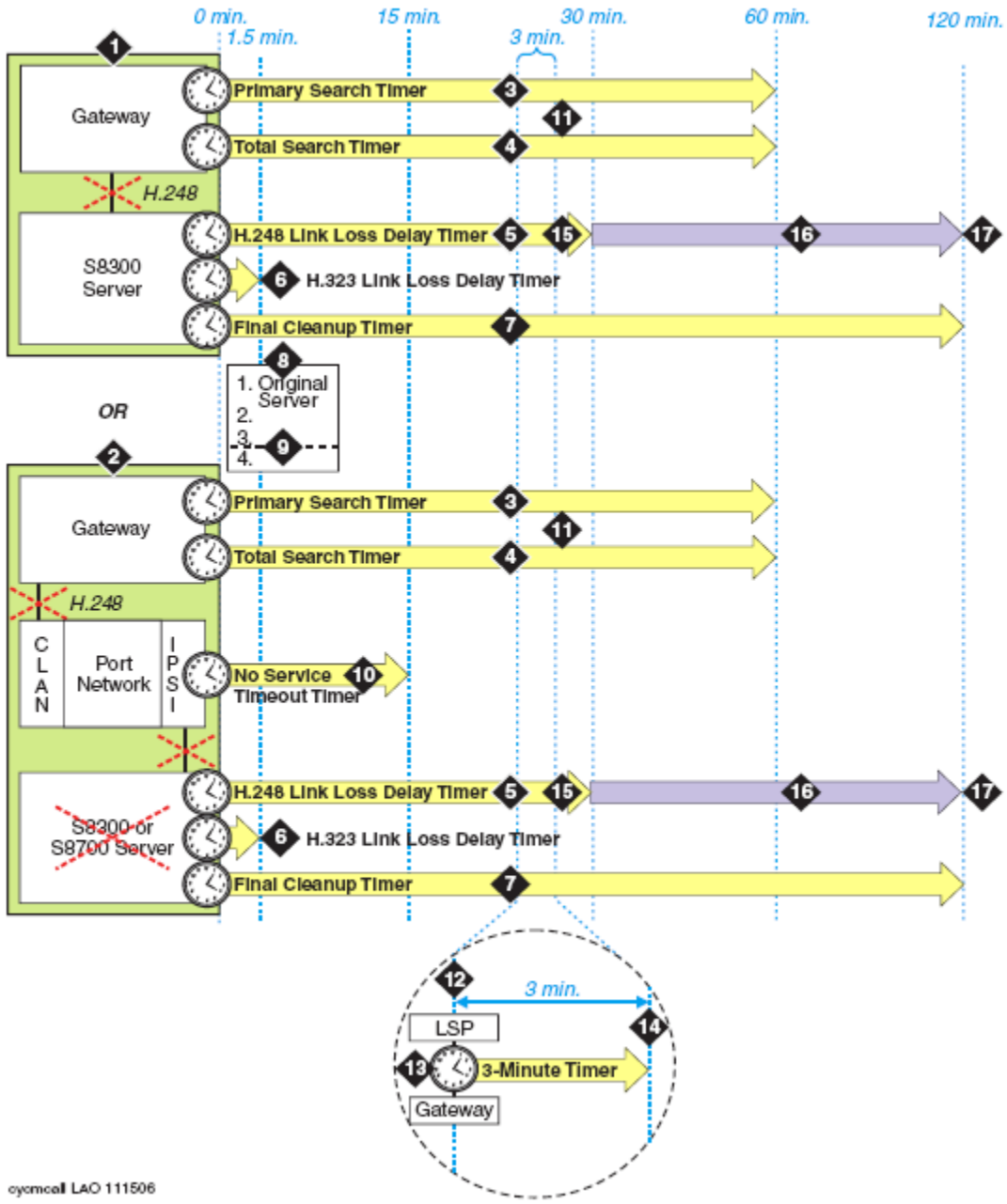


Figure 6: Recovery timers and interactions

Numbers	Description
1	S8300D: H.248 link between the server and the gateway is broken.

Numbers	Description
2	**S8510 Server** (Processor Ethernet interface) or Duplicated server series: If the Ethernet connection is broken between the server and the port network or the server fails, the Survivable Core Server on page 98 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 Link Recovery design on page 78) begins on the gateway.
4	Total Search Timer (TST, see Link Recovery design on page 78) begins on the gateway.
5	Link Loss Delay Timer (1-30 min.) starts when Communication Manager detects loss of connection with a gateway.
6	H.323 Trunk Link Recovery on page 94 starts a short (1.5 min.) timer to hold the call state information for H.323 (IP) trunks.
7	Final Cleanup Timer (120 min.) cleans up preserved connections that do not have disconnect supervision.
8	Media Gateway Controller list (MGC). The first element in this list is always the primary server; the fifth element is for G450 SLS (survivable-call-engine).
9	Transition point (see Note 8 and Administrating the Media Gateway timer on page 83)
10	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.
11	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.
12	Auto Fallback to Primary starts a 3-minute, administrable timer that checks for network stability before the server accepts the registration requests from the gateway.
13	Auto Fallback to Primary on page 96: depending upon its recovery rule, the gateway connects to Survivable Remote Servers before the Link Loss Delay Timer (LLDT) expires.
14	Auto Fallback to Primary on page 96: gateway sends registration requests to primary server at 30-second intervals (similar to keep alive signals). Server

Numbers	Description
	gives gateways without Survivable Remote Servers service priority to those with Survivable Remote Servers service; see Survivable Remote Servers on page 97.
15	Link Loss Delay Timer (LLDT) expires, Connection Preserving failover and failback on page 75 and Standard Local Survivability (SLS) on the G450 Branch Gateway and G430 Branch Gatewayand J4360/J6350 gateways begin.
16	Connection Preserving failover and failback on page 75 starts as soon as the gateway migrates to another server.
17	Connection Preserving failover and failback on page 75 Final Cleanup Timer (FCT) expires.

Connection preserving failover and failback

The Connection Preserving failover and failback for gateways preserves existing bearer (voice) connections while a branch 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. In addition to preserving the audio voice paths, Connection Preserving failover and failback extends the time period for recovery operations and functions.

If two parties are on a call that is routed through a branch 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 permitted. Avaya's network recovery strategy includes the Connection Preserving failover and failback feature to ensure that the new server to which the gateway connects retains calls in progress.

Conditions that initiate Connection Preserving failover and failback

Connection Preserving failover and 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 and failback preserves the voice path after it migrates to the new server. Loss of the H.248 network connection causes the gateway to failover or failback to a new server:

- Main server to Survivable Remote Servers or Survivable Core Server
- Main server back to itself after system reset
- One Survivable Remote Servers to another Survivable Remote Servers
- One Survivable Core Server to another Survivable Core Server

- Survivable Remote Servers to a Survivable Core Server
- Survivable Remote Servers/Survivable Core Server back to main server after expiration of the Link Loss Delay Timer that clears out calls on the server.

Types of calls

Connection Preserving Failover/Failback preserves:

- Stable calls (talk path already established) originating from the main server, including:
  - Analog stations and trunks
  - DCP stations
  - Digital trunks
  - IP trunk calls (SIP, H.323)
  - H.323 IP stations that use gateway resources
  - ISDN-PRI trunks
    - D-channel on the 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 gateways. Avaya recommends that the gateways be physically co-located and administered to migrate together to the same set of Survivable Remote Servers 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

Important:

Call features, such as Hold, Transfer, Drop 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 and Failback does not preserve:

- Preserved calls (originating on the main server) on a Survivable Remote Servers that falls back to the primary server. Calls that originate on the Survivable Remote Servers during the time period that it is providing call control are preserved when the Survivable Remote Servers fails back to the primary server.

Important:

If you want calls that originate on the main server to remain stable throughout the failover and failback process, that is, when the Survivable Remote Servers falls back to its assigned primary server, ensure that the gateways recovery rule (**`change`**

system-parameters mg-recovery-rule n, **Migrate H.248 MG to primary** field) is set to:

- 0-active calls which causes the Survivable Remote Servers to failback to the primary server when the system is idle (no active calls in progress)
- time-day-window which specifies a time for the Survivable Remote Servers failback to the primary server.
- time-window-OR-0-active-calls which fails back to the primary server whenever the system is idle or at the administered time, whichever occurs first.

- Calls on hold or listening to announcements or music (not considered stable calls).
- ISDN BRI calls
- 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

H.248 server-to-gateway Link Recovery

The H.248 link between an Avaya server running Communication Manager Software and the Avaya 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 Survivable Remote Servers. Link Recovery does not diagnose or repair the network failure that caused the link outage.

Link Recovery begins with detection of either:

- A TCP socket failure on the H.248 link

  or

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

Link recovery design

Link recovery design incorporates three separate timers that monitor the period of time that the server or gateway spends in specific link recovery processes. The table on page 78 lists the timer parameters.

Table 26: 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)
Final Cleanup Timer	Server	Removes preserved connections that do not have disconnect supervision (not administrable).	120
Primary Search Timer	Gateway	The length of time that the gateway spends trying to connect to the primary server.	1-60(1)
Total Search Timer	Gateway	The length of time that the gateway spends trying to connect to all alternate resources.	1-60(30)

The sequence of events during Link Recovery is described in the table on page 78.

Table 27: General Link Recovery process

Process sequence	Description
1.	Link failure detected
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 83 for instructions on administering this list. See Administrating the Media Gateway timer on page 83 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: S8300D: 1-3 S8300Dconfigured as Survivable Remote Server. S8510 Server and Duplicated servers: 1-3 C-LAN circuit packs within the primary server's configuration

Process sequence	Description
	The Total Search Timer continues running. See Administering the MGC list on page 83 for instructions on administering this list and on setting the Transition Point.
4.	If the Primary Search Timer expires before the gateway can re-establish the link to the alternate resources that are above the Transition Point in the MGC list, then the gateway crosses the Transition Point and begins searching the other resources in the list. The gateway makes 2 connection attempts with any resources below the Transition Point: one on the encrypted link, the other on the unencrypted link.
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, it reboots itself. For more information on the server and gateway alarm notification strategies, see Maintenance during recovery on page 80. 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 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 to another server.

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.
  - G450 Branch Gatewayand G430 Branch Gateway reboots after the Total Search Timer expires.
  - Media modules reboot after the Total Search Timer expires.
- 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.
- Telephone buttons (including feature access buttons) do not work.

The Feature interactions and compatibility on page 84 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 the table on page 80.

Table 28: Communication Manager alarms

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

Gateway alarms

The Gateway events, their associated alarm levels, and SNMP status are listed in the table on page 81.

Table 29: Gateway events and alarms

Event	Alarm level	Log	SNMP
Loss of link	Minor	Event	Trap
Link restored	Cleared	Event	Trap clear
Registration successful	Informational	Event	Trap
Registration failed	Major	Event	Trap
No controller provisioned	Major	Event	Trap
Controller provisioned	Major	Event	Trap clear
Connection to Survivable Remote Servers	Major	Event	Trap
Connection fallback to primary	Major	Event	Trap clear

Note:

Communication Manager raises a minor alarm until the Link Loss Delay timer expires. If the link to the original gateway is restored before this timer expires, then the alarm is cleared. If the Link Loss Delay Timer expires but the gateway successfully connects with a Survivable Remote Servers, the main server generates a warning alarm anyway, even though the H.248 link is up to another server.

Administering the server timer

About this task

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. Use this procedure to administer the Link Loss Delay Timer.

Procedure

1. At the SAT type **`change system-parameters ip-options`** and press `Enter`to display the IP-Options System Parameters form (the figure on page 82).

```
change system-parameters ip-options
                                                              Page   1 of   4
                           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
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
   Server IPV4 Address:                  RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                        H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                     Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5          Primary Search Time (sec): 75
                                  Periodic Registration Timer (min): 20
                               Short/Prefixed Registration Allowed? n
```

Figure 7: IP-Options System Parameters form

2. In the H.248 MEDIA GATEWAY section type a number (1–30; default is 5) in the **Link Loss Delay Timer (minutes)** field to indicate 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 (Primary Search Timer and Total Search Timer. See Administrating the Media Gateway timer on page 83).

3. Press `Enter` to save the change.

Media Gateway timers administration

Administering the Media Gateway requires you to administer the Primary Search Timer, the Total Search Timer, and the MGC list Transition Point. The MGC Transition point divides the MGC list into two categories:

- Elements above the Transition Point are alternative C-LAN circuit packs connected to the primary server.
- Elements below the Transition Point can be other C-LAN circuit packs or Survivable Remote Servers on branch gateways.

Administrating the Media Gateway timer

About this task

Use this procedure to administer the gateway timers and Transition Point.

Procedure

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 78 for more information about the H.248 Link Recovery timers.

Administering the MGC list

About this task

You can administer the gateway with a list of up to 4 alternate resources (TN799DP C-LAN circuit packs or Survivable Remote Servers) 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.

Use this procedure to administer the MGC list.

Procedure

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 (S8300D) or the primary C-LAN circuit pack (Duplicated servers).
   - The next three elements can be the IP addresses of 1-3 Survivable Remote Servers (S8300D configured as such), other C-LAN circuit packs in the primary server's configuration (Duplicated servers), or the Standard Local Survivable call engine on branch gateways.
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 (the table on page 84).

Table 30: H.248 Link Recovery feature/adjunct interactions

Feature or adjunct	Description
Feature Access Codes (FAC)	Feature Access Codes, whether dialed or administered buttons, do not work.
Non-IP trunks/stations, including such circuit-switched TDM resources as DCP, analog, or ISDN-PRI.	These resources are unavailable until the H.248 link is re-established.
Terminals	Time-of-Day, busy lamp states, and call appearance status on some phones might not instantaneously reflect the correct information until the H.248 link is re-established.
Adjunct Switch Application Interface (ASAI)	ASAI-based applications that use timing loops, time-related methods, or events might not perform as intended. In addition, applications that do not accommodate time-outs or missing state transitions might behave unpredictably.
Voice mail adjuncts (Communication Manager Messaging application)	During Link Recovery, callers connected to the Communication Manager Messaging application

Feature or adjunct	Description
	remain connected even if they stop responding. Such calls might be automatically disconnected by the Communication Manager Messaging application if the connection remains intact without the calling party entering tone commands to the Communication Manager Messaging application or voicing a message.
Call Detail Recording (CDR)	Call records cannot reflect the correct disconnect time if the calling party hangs up before the link recovers.
Call Management System (CMS)	Measurements collected during the recovery period might be inaccurate in those reports that rely upon time-related data.
Property Management System (PMS)	Automatic Wake-up, Daily Wake-up, and Housekeeping Status features might not operate as expected if the link fails and the time to search for alternate resources exceeds the PMS application's time-out parameters. 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 use timing loops, time-related methods, or events might not perform as intended. In addition, applications that do not accommodate time-outs or missing state transition(s) might behave unpredictably.

Network fragmentation

A likely outcome to an H.248 link recovery scenario is that a network of gateways and IP endpoints, initially registered to the primary server, might now be registered to a number of different Survivable Remote Servers 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 gateways that are not registered with the primary server. If the technician is on site, the illumination of the YELLOW ACT LED on the Survivable Remote Servers is an indication that something has registered with that Survivable Remote Servers, and therefore, that the network is fragmented. Two methods are available to recover from a fragmented network:

- Auto Fallback to Primary on page 96 describes how this feature reconstructs the server/gateway topology following network fragmentation.
- Execute **reset system 4** on each Survivable Remote Servers.

  To force 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 Survivable Remote Servers 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.

  The only way to be certain that gateways and endpoints re-register with the primary server is to shut down Communication Manager on every Survivable Remote Servers in the network.

Restarting and shutting down Communication Manager on every Survivable Remote Servers

About this task

Use this procedure to shut down or restart Communication Manager on every Survivable Remote Servers.

Procedure

1. At each Survivable Remote Servers command line type **stop -acfn** and press Enter.
2. Disable the processor ethernet interface (**procr**).
3. At the primary server's SAT type either **list media-gateway** or **status media-gateway** and press Enter.
4. Verify that all the network endpoints re-registered with the primary server.
5. At each Survivable Remote Servers command line type **start -ac** and press Enter to restart Communication Manager on each Survivable Remote Servers.

H.323 Link Recovery

The H.323 link between an Avaya 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 Survivable Remote Servers.

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.

Synopsis of recovery outcomes are mentioned below:

- If no gateway is found, the endpoint is out-of-service until it can find a Gateway.
- If IP endpoint registers with a new gateway, the call ends and the endpoint is available (full features and buttons) through the new gateway.
- If 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

Link recovery sequence

The sequence of events during recovery and an explanation of what it happening is listed below. This sequence correlates with H.323 Link Bounce recovery process on page 89.

1. If one of the following link failure detected:
    - 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).

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 the figure on page 89).
3. 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.
4. 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 on page 90. 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.
5. 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 the figure on page 89).
6. 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.
7. 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 on page 90. 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.

8. 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.

9. 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 (the figure on page 89) has not expired yet.
10. If the connection cannot be established with an address(es) of the primary Gateway or if the Primary Search Time (Note 3 in the figure on page 89) has expired, the endpoint then tries to register with the address(es) of the next Gateway in the Alternate Gateway List on page 90, as depicted by Note 8 in the figure on page 89).
11. The endpoint continues its re-registration attempts, as depicted by Note 9 in the figure on page 89.
12. When the H.323 Link Loss Delay Timer expires (Note 10 in the figure on page 89), the Gateway drops all call state information.

Link bounce recovery process

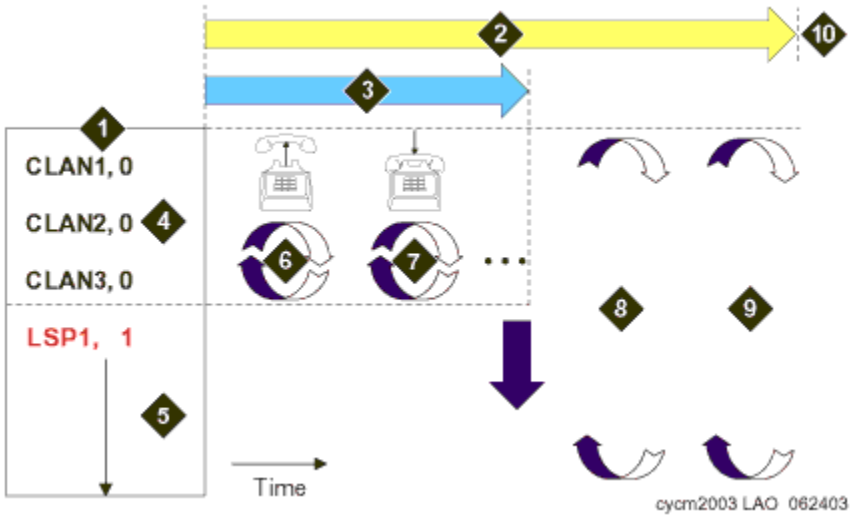


Figure 8: H.323 Link bounce recovery process

Number	Description
1	Alternate Gateway List
2	H.323 (gateway) Link Loss Delay Timer
3	Primary Search Timer (endpoint)
4	IP address of alternate C-LAN and Gateway ID
5	Survivable Remote Server list in search order.

Number	Description
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 Survivable Remote Server.
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.

The figure on page 89 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 a Survivable Remote Servers, followed by a Gateway ID. The purpose of the ID is to differentiate the C-LAN addresses from a Survivable Remote Servers 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 the figure on page 89) contains the IP address of a Survivable Remote Servers). The single entry implies that there is only one Survivable Remote Servers 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.

H.323 Link Recovery 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.

Administering H.323 Link Recovery

About this task

Use this procedure to administer H.323 Link Recovery options.

Procedure

1. At the primary server SAT type change system-parameters ip-options and press Enter to display the IP Options System Parameters form.

```
change system-parameters ip-options                          Page   1 of   4
                          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
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
   Server IPV4 Address:                 RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005
AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                      H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                   Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5        Primary Search Time (sec): 75
                                 Periodic Registration Timer (min): 20
                               Short/Prefixed Registration Allowed? n
```

2. Set the number of minutes for Link Loss Delay Timer, Primary Search Timer, and **Periodic Registration Timer** fields.
3. At the primary server SAT type **change ip-network-region n**, where **n** is the Network Region number, to display the IP Network Region form.

```
change ip-network-region 1                                   Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1               Authoritative Domain:
    Name:
                                Intra-region IP-IP Direct Audio: yes
MEDIA 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
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
       Vidio 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: 46
```

4. Administer the H.323 Link Bounce Recovery, Idle Traffic Interval, Keep-Alive Interval, and **Keep-Alive Count** fields.

IP-Option System Parameter field descriptions

Name	Description
Link Loss Delay Timer (min)	The range for this field must be 1- 60 and the default value is 60.
Primary Search Time (sec)	The range for this field must be 5-3600 and the default value is 75.
Periodic Registration Timer (min.)	The range for this field must be 1-60 and the default value is 60.
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.

Name	Description
	The need for this timer arises in situations where the current Communication Manager server might have a large number of C-LANs. Using this timer, the customer can specify the maximum time that an IP endpoint spends on trying to connect to the C-LANs before attempting to register with a Survivable Remote Servers. 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 telephone's registration is taken over by another IP endpoint. The timer is cancelled upon successful RAS registration. When the timer expires, the telephone 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 Regions field descriptions

Name	Description
Idle Traffic Interval[Endpoint]	The maximum traffic idle time after which a TCP Keep-Alive (KA) signal is sent from the endpoint. Range: 5-7200 seconds

Name	Description
	Default value: 20
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. Range: 1-120 seconds Default value: 5
Keep-Alive Count[Endpoint]	The number of times the Keep-Alive message is transmitted if no ACK is received from the peer. Range: 1-20 Default value: 60
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.]

H.323 Trunk Link Recovery

By initiating a timer to hold the call state information the H.323 Trunk Link Recovery feature results in fewer call failures caused by IP network failures or disruptions. Communication Manager preserves calls and starts a timer at the onset of network disruption (signaling socket failure):

- If the signaling channel recovers before the timer expires, all call state information is preserved and the signaling channel is recovered.
- If the signaling channel does not recover before the timer expires, the system
  - raises an alarm against the signaling channel
  - maintains all connections with the signaling channel
  - discards all call state information about the signaling channel

Administering H.323 Trunk Link Recovery

About this task

Use this procedure to administer H.323 trunk link recovery.

Procedure

1. At the SAT interface, type **list signaling-group** and press Enterto display a list of the administered signaling groups. Find the H.323 signaling group(s) in the list.
2. Type **change signaling-group n**, where **n** is an administered H.323 signaling group.

```
display signaling-group 2
Page   1 of   6
                                SIGNALING GROUP
 Group Number: 2              Group Type: h.323
 SBS? n                   Remote Office? n        Max number of NCA TSC: 10
 Q-SIP? n                                           Max number of CA TSC: 0
 IP Video? n                                     Trunk Group for NCA TSC: 2
    Trunk Group for Channel Selection: 2       X-Mobility/Wireless Type:
NONE
   TSC Supplementary Service Protocol: a          Network Call Transfer? n
  Location for Routing Incoming Calls:                 T303 Timer(sec): 10
H.245 DTMF Signal Tone Duration(msec):
     Near-end Node Name: procr                   Far-end Node Name: S8300
 Near-end Listen Port: 1720                Far-end Listen Port: 1720
                                         Far-end Network Region: 1
        LRQ Required? n              Calls Share IP Signaling Connection? y
         RRQ Required? n
    Media Encryption? n                  Bypass If IP Threshold Exceeded? n
                                                 H.235 Annex H Required? n
        DTMF over IP: out-of-band          Direct IP-IP Audio Connections?
y
  Link Loss Delay Timer(sec): 90                     IP Audio Hairpinning? y
       Enable Layer 3 Test? y                Interworking Message: PROGress
H.323 Station Outgoing Direct Media? n   DCP/Analog Bearer Capability:
3.1kHz
```

3. Type the number of seconds to retain the call state information in the **Link Loss Delay Timer** field (1-180 seconds, default is 90).
4. If you want Communication Manager to run the Layer 3 test that verifies that all connections known at the near-end are recognized at the far-end, type **y** in the **Enable Layer 3 Test** field.

Note:

The default value is **y** (test enabled), however some systems, possibly older Communication Manager releases, respond incorrectly to this test. Set the value to **n** in these cases. If this field is administered as **y** (test enabled) and the **Far-end Node Name** does not have an administered IP address, then you cannot submit the form.

Note:

The **Far-end Node Name** must have an administered IP address, otherwise the Layer 3 test aborts.

5. Press Enter to save the changes.

Auto Fallback to Primary

The intent of this feature is to return a fragmented network, where a number of branch gateways are being serviced by one or more Survivable Remote Servers, to the primary server in an automatic fashion. This feature is targeted towards all branch gateways. The main driving force for this feature is the fact that, when a gateway is receiving service from a Survivable Remote Servers, the notion of the big single distributed switch is no longer the case; therefore, resources are not being used efficiently. By migrating the gateways 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 a gateway 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 gateway and the server side is the Communication Manager server. The client actively attempts to register with the primary server while it maintains its H.248 link to the Survivable Remote Servers. This is being done, so that the server can permit a registration or deny it. When a gateway is being serviced by a Survivable Remote Servers, then the Primary Server has the option to deny a registration in cases where the server may be overwhelmed with call processing, or based upon system administration.

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

Using this feature, the administrator can define any of the following rules for migration:

- The gateway should migrate to the primary automatically, or not.
- The gateway should migrate immediately when possible, regardless of active call count.
- The gateway should only migrate if the active call count is 0.

- The gateway should only 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 gateway 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 is adjustable to fit the recovery strategy.

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

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

Survivable Remote Servers

S8300D and S8510 Server (through the Processor Ethernet interface) Servers can act as a survivable call-processing servers for remote or branch customer locations. As Survivable Remote Servers, they have a complete set of Communication Manager features, and using its license file, it functions as a survivable call processor. If the link between the gateways and the primary controller is broken, those telephones and gateways that are designated to receive backup service register with the Survivable Remote Servers. The Survivable Remote Servers provides control to those registered devices in a license error mode, see Avaya Aura® Communication Manager Hardware Description and Reference, 555-245-207.

Returning an active Survivable Remote Servers to standby mode

About this task

When the primary server is available again, it begins handling calls, however, for configurations earlier than Release 3.0 (Auto Fallback to Primary on page 96 feature returns active Survivable Remote Servers to standby mode) endpoints that were registered with the Survivable Remote Servers stay registered until the Survivable Remote Servers is rebooted.

Caution:

This procedure reboots the Survivable Remote Servers, dropping all calls. Ensure that you perform this procedure from the Survivable Remote Servers, not the active server.

Use this procedure to return an active Survivable Remote Servers to standby mode:

Procedure

1. Log in to **System Management Interface**.
2. Click **Administration** > **Server (Maintenance)**.
3. Click **Server** > **Shutdown Server**.
   The Shutdown Server page displays.
4. 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.
5. Select the **Restart server after shutdown** check box.
6. Click **Shutdown**.
7. Verify that all the gateways have re-registered with the main server.
8. Log back on to the Survivable Remote Servers through SAT interface for the Survivable Remote Servers.
9. Type **`status media-gateway`** to display the GATEWAY STATUS page.
10. 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.

Survivable Core Server

In the gateway architecture today, gateways register with a primary call controller; however, the IP interface through which the gateway registers can either be on the call controller directly in the case of S8300D Server, or through a C-LAN interface in the case where the call controller is a Duplicated server series or S8510 Server (through the Processor Ethernet interface).

The Survivable Core Server feature provides survivability to Port Networks. Using the Survivable Core Server feature, backup servers can be placed in various locations in the customer’s network. The backup servers supply service to Port Networks in the case where the S8510 Server, or the Duplicated series server pair fails, or connectivity to the main Communication Manager server is lost. Survivable Core Servers can be either S8510 Server or Duplicated series servers, and offer full 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 a Survivable Core Server cannot control a Center Stage Switch.

When designing a network to support Survivable Core Servers, consider the following:

- Survivable Core Servers can only control Port Networks that they can reach over an IP network. That is, Survivable Core 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:
  - Survivable Core Servers 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 Survivable Core Servers can be deployed in a network. In the case above, an enterprise could deploy one or more Survivable Core Servers 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 Survivable Core Servers, system fragmentation may occur. In that case, users should take care to establish adequate trunking and routing patterns at a particular location to be able to place calls where needed.
- Survivable Core Servers register to the main server(s) through a C-LAN. Each Survivable Core Servers must be able to communicate with a C-LAN to download translations.

The gateway cannot distinguish between registration through a C-LAN or registration to a server directly. Prior to Communication Manager 3.0, without Survivable Core Servers, if a gateway successfully registered with a primary call controller IP address, then the gateway was properly registered with the primary call controller. However, in Communication Manager 3.0 and later, when a gateway completes a successful registration through an IP address defined as a primary call controller address, if that address is a C-LAN, the 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 a Survivable Core Servers; but the gateway will not know that it is registered with a Survivable Core Servers.

When the traditional port network migrates back to the primary call controller, then the 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 gateway drops the connection and registers with a Survivable Remote Servers. The Survivable Core Servers migration should only occur if the port network is reasonably certain to return to the primary call controller, so the gateway would simply return to the same C-LAN interface. Now, when the 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 gateway. The controller in this case issues a warm start request to the gateway, or potentially different behavior if connection preservation is active at the same time. The Auto-Fallback feature is not affected by Survivable Core Servers.

For more information on survivable core servers, see *Avaya Aura® Communication Manager Survivable Options*.

WAN Remoted Port Network

With the trend toward convergence, more customers have been remoting their port networks (PN is located across WAN from the Communication Manager server). The timing requirements on the port network to Communication Manager are very tight and assume traditional closed networks. WAN disruptions are much more frequent than those in traditional closed networks and can take more than several seconds for recovery, even in well-managed networks. Communication Manager maintenance and the Packet Control Driver (PCD) traditionally begin taking recovery action after three seconds. Using the Administrable IPSI Socket Sanity Timeout, you can get an extension of 3 to 15 seconds before the system initiates recovery action. The IPSI socket sanity timeout is administrable on the system-parameters ipserver-interface form. The default is 15 seconds.

The timeout extension will lessen the impact of network failures by postponing port network recovery action after a network outage and give time for the network to recover. If the network does recover within that time, call control can resume with minimal disruption.

The IPSI socket sanity timeout value would typically be administered at the main site only. In a duplicated server pair, the value is part of translations, which are filesync'd to the standby server, as well as to all Survivable Core Servers in the system.

The Survivable Core Servers can be administered independently and temporarily when it is active, but all such translations are lost as soon as the main returns to service and updates translations, or there is a manual **`reset system 4`**. Likewise, the IPSI socket sanity timeout value can be administered on an active Survivable Core Servers, but its value will be overwritten once the main returns to service and updates translations.

For Simplex IPSIs, if there is no alternative control path available, the timeout is extended to the customer value.

The various duplication and alternate path conditions are shown in the table on page 100, along with the associated recovery action.

Interactions/Alternate Paths

Table 31: Interactions / Alternate Paths

System Conditions	Recovery Action	Resets / Restarts
Simplex IPSIs on IP Port Networks: Socket gets to 3 seconds without heartbeats acknowledged or no data received.	IPSI socket timeout extends to customer set value.	PKTINT reset and PN warm restart expected if socket timeout reached and socket re-established before warm restart timeout.

System Conditions	Recovery Action	Resets / Restarts
Duplicate IPSIs on IP Port Networks: Both sockets get to 3 seconds without heartbeats acknowledged or no data received.	Both IPSI socket timeouts extend to customer set value.	PKTINT reset and PN warm restart expected if socket timeout reached and socket re-established before warm restart timeout.
Duplicate IPSIs on IP Port Networks: Active socket goes to 3 seconds without heartbeats acknowledged, but standby socket heartbeats are acknowledged.	Spontaneous IPSI interchange. Neither timeout is extended, since there is a viable “alternate path” for the control links.	Ideally, none. Previous failing Active IPSI board reset.
Duplicate IPSIs: Standby socket gets to 3 (or more) sanity failures, but active has no sanity failures.	Neither timeout is extended.	None. Standby PKTINT reset when re-established.
Fiber connected PNs with Simplex IPSIs: If some IPSI sockets get to 3 seconds without heartbeat acknowledged, but at least one IPSI has heartbeats acknowledged.	Maintenance software will migrate the control links to the EIs in the PNs where the IPSIs have lost IP connectivity. None of the IPSI socket sanity timeouts are extended, since there are viable “alternate paths” for the control links.	PN warm reset and PKTINT reset on failing IPSIs when socket re-established.
Fiber connected PNs with duplicated IPSIs: Active socket goes to 3 seconds without heartbeats acknowledged, but standby socket heartbeats are acknowledged.	Spontaneous IPSI interchange. Neither timeout is extended, since there is a viable “alternate path” for the control links. Maintenance software will migrate the control links to the EIs in the PNs where the IPSIs have lost IP connectivity. None of the IPSI socket sanity timeouts are extended, since there are viable “alternate paths” for the control links.	PN warm reset and PKTINT reset on failing IPSIs when socket re-established.
Fiber connected PNs, with IPSIs: If all IPSI sockets get to 3 seconds without heartbeats acknowledged.	All IPSI socket sanity timeouts will extend to customer set value.	PKTINT reset and PN warm restart expected if socket timeout reached.

Chapter 4: General troubleshooting

This section contains information to help you understand system problems reported through maintenance subsystem of Communication Manager. While pro-actively testing in the background, gathering and reporting vital information from several concurrent processes, Communication Manager maintenance can often notify you of problems before failures like variations in environments (temperature, voltages, fan speeds), and of irregularities in connections or services occur. While resolving the problem you must 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. After the location is identified, repair the problem by correcting parameter provisioning, upgrading software or firmware, or replacing hardware.

Commonly-accessed directories and files on Linux servers

The table on page 103 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 the table on page 103.

Table 32: Directories and files for troubleshooting

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 System Management Interface (SMI). 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 SMI.

Directory	File	Description
/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 SMI.
	lspList	This file is usually 0 bytes long, unless one or more Survivable Remote Servers are registered to this server. If Survivable Remote Servers are registered, this file contains the IP addresses of the Survivable Remote Servers to which Communication Manager has tried to send the translation files. This file is populated by registering Survivable Remote Servers.
/var/log/ecs		This directory contains three very useful types of files: • ecs log files on page 104 • Commandhistory on page 104 • wdlog on page 104
	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 on page 104 for some

Directory	File	Description
		basic information about core dumps. This file is populated by various Linux processes.
/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 on page 104 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.

Identify the problem

Having the answer to the following question determines whether or not you can benefit from the information that follows in this section:

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 identify the 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 servers, media modules, and circuit packs have color-coded LEDs to indicate the presence of alarms and the level. See *LED Descriptions for Avaya Aura® Communication Manager Hardware Components*, 03-602804.
- Avaya phones can have administered buttons to indicate certain types of alarms. See *Administering Avaya Aura® Communication Manager*, 03-300509.

User-reported problems

Telephone 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.

Checklist for resolving a user reported problem

You must collect the following information when you receive notification of a problem from a user within the system.

Requirements	Value	Notes
User location		
User extension		
Is anyone else experiencing this problem?		
What kind of call was made?		
Whom was the call made to?		
When was the call made?		
Is the problem reproducable?		

Resolving a user reported problem

About this task

Use this procedure to resolve a reported problem of a user within the system.

Procedure

1. After you have collected the required information about the reported problem. Look up connection/configuration information (**`status station`**) as shown in the figure on page 108 through the figure on page 109.

   Note:

   Different fields might appear on this screen, and some fields might appear on different pages depending on your system configuration. The figure on page 108 is an example only.

```
status station 5141013                                        Page   x of   x
                              GENERAL STATUS
     Administered Type: 9640SIP            Service State: in-service/on-hook
        Connected Type: N/A
             Extension: 514-1013
                  Port: S00001        Parameter Download: complete
           Call Parked? no                SAC Activated? no
      Ring Cut Off Act? no
Active Coverage Option: 1            one-X Server Status: N/A

          EC500 Status: N/A       Off-PBX Service State: in-service/idle
   Message Waiting:
   Connected Ports:


  Limit Incoming Calls? no

 User Cntrl Restr: none                        HOSPITALITY STATUS
Group Cntrl Restr: none                      Awaken at:
                                              User DND: not activated
                                             Group DND: not activated
                                           Room Status: non-guest room
```

Figure 9: Status station form, page 1

2. Perform the following to resolve the issue:
   a. Ensure that the value in **Service State** field is in-service.
   b. Check the extension number in the **Extension** field.
   c. Write down the Port assignment.
   d. Scroll to the GENERAL STATUS section of the form.

```
status station 5141013                                        Page   x of   x
                                GENERAL STATUS

CONNECTED STATION INFORMATION
               Part ID Number: unavailable
                Serial Number: unavailable

          Station Lock Active? no            TOD Station Lock: no

CF Destination Ext:

Enhanced Call Forwarding Destination
                 Internal                  External
  Unconditional:
           Busy:
       No Reply:
```

Figure 10: Status station form, page 2

   e. If the user-report is that the station cannot be called or does not ring, ensure the following:
      - Ensure that the **CF Destination Ext** field is blank.
      - Ensure that the **SAC Activated** field is set to no.

- Ensure that the **Ring Cut Off Act** field is set to no.
- Ensure that the**User Cntrl Restr** and **Group Cntrl Restr** fields are set to none. This controlled station restriction can render the station outgoing- or incoming-restricted, or completely disabled (both outgoing- and incoming-restricted).
- Ensure that the **User DND** and **Group DND** options are not activate.

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 UNICODE DISPLAY INFORMATION section of the form.

```
status station 5141013                                          Page   x of   x
                        UNICODE DISPLAY INFORMATION

          Native Name Scripts: 0x00000001:Latn
      Display Message Scripts: 0x06000001:Jpan;Kana;Latn
    Display Message 2 Scripts: 0x00000001:Latn
    Display Message 3 Scripts: 0x00000001:Latn
    Display Message 4 Scripts: 0x00000001:Latn
    Station Supported Scripts: 0x00000007:Latn;Lat1;LatA
```

Figure 11: Status station form, page 3

h. Scroll to ATM VPI.VCI DATA section of the form.

```
status station 5141013                                          Page   x of   x

                                ATM VPI.VCI DATA

 Port         Talk            Connected Port         Listen

 S00002       n/a
```

Figure 12: Status station form, page 4

i. Scroll to CALL CONTROL SIGNALING section of the form.

```
status station 5141013                                          Page   x of   x
                              CALL CONTROL SIGNALING
Port: S00002         Switch-End IP Signaling Loc:          H.245 Port:
            IP Address                                Port  Node Name       Rgn
Switch-End:  135.122.47.152                           1720   mc_clan2       1
Reg Set End:
Alt Set End:
H.245 Near:
 H.245 Set:
```

Figure 13: Status station form, page 5

j. If this is an IP endpoint, note down Switch Port, Switch-End IP Address:Port, and **Set-end IP Address:Port** fields information.

k. Scroll to Audio section of the form.

```
status station 5141013                                          Page   x of   x

                          AUDIO CHANNEL Port: S00002
              Switch-End Audio Location:
            IP Address                                Port  Node Name       Rgn
Other-End:
  Set-End:
Audio Connection Type: ip-tdm
```

Figure 14: Status station form, page 6

l. Check the **Audio Connection Type** field (ip-tdm).

m. Scroll to IP ENDPOINT DATA section of the form.

```
status station 5141013                                          Page   x of   x

                          IP ENDPOINT DATA
                  Port: S00002
 Product ID-Release:                            H.245 Tunneled? does not apply
Registration Status: registered-authenticated      MAC Address:

 Native NAT Address:
ALG NAT WAN Address:
```

Figure 15: Status station form, page 7

n. Check the **Registration Status** field (registered-authenticated).

o. Scroll to ACD STATUS section of the form.

```
status station 5141013                                          Page   x of   x

                                   ACD STATUS

 Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod
    /        /        /        /        /        /        /    On ACD Call? no
    /        /        /        /        /        /        /
    /        /        /        /        /        /        /     Occupancy: 0.0
    /        /        /        /        /        /        /
```

Figure 16: Status station form, page 8

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 the table on page 111 along with their usage.

Table 33: Troubleshooting commands and description

Command	Description
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	Using this command, an administrator can 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, keep alive, 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.

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 the following 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.

The maintenance subsystem gathers detailed alarm and error information from three major processes:

- Communication Manager— the telephony application
- Server-based maintenance subsystem applications
- Linux server

You can view the Alarm Log through any of the three different interfaces listed in the table on page 112.

Table 34: 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 on page 119 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 start an: • Filtering event report on page 118: logs and explains specific events that occur during call processing. Often, these are not problems that require immediate action, but are informational. • Filtering alarm report on page 116: the main source for Communication Manager alarms, which include out-of-range temperature or voltage values,

Interface	Connection	Description
		broken or fluctuating connections, defective hardware, etc.
Command Line Interface (CLI)	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 103 for information about the types of files and logs and their locations.

Maintenance subsystems

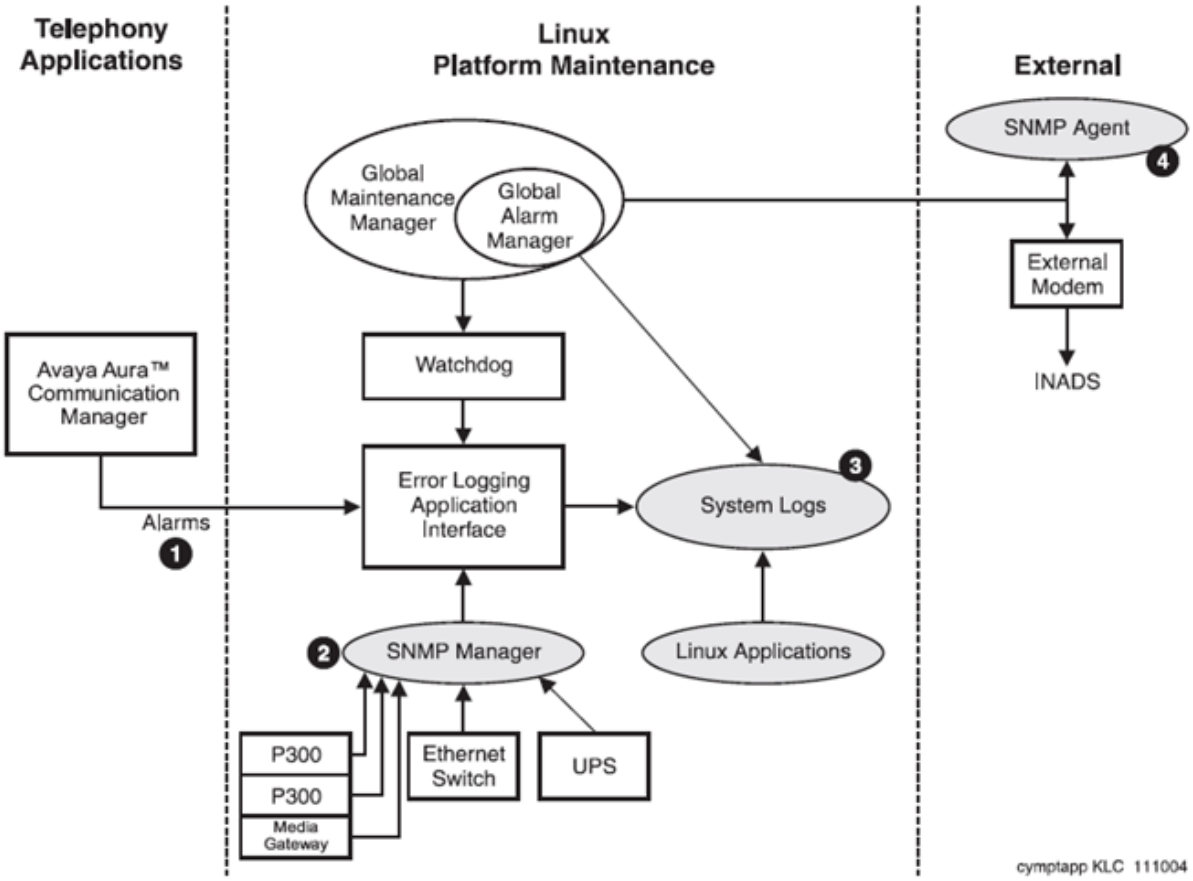


Figure 17: Maintenance subsystems

Number	Description
1	Communication Manager alarms

Number	Description
2	SNMP Manager sends traps to SNMP Agent application
3	System logs
4	SNMP Agent application

Current alarms

The figure on page 115 shows an example of an alarm log as seen from System Management Interface.

Current Alarms

The Current Alarms SMI page provides a list of alarms and their origin. Alarms are listed in chronological order beginning with the most recent. Alarms cannot be viewed unless the telephony application is running.

Product ID: "1000000000"

ALARM CATEGORIES	MINOR	MAJOR
Server	Yes	No
CommunicaMgr	Yes	No

CommunicaMgr Alarms

ID	MO	Source	On Bd	Lvl	Ack	Date
1	MG-ANA	001V2	y	MIN	Y	Mon Jan 23 15:59:41 IST 2012
2	UDS1-BD	01B08	y	MIN	Y	Mon Jan 23 15:56:09 IST 2012
3	SP-REG-M	NUL	n	MIN	Y	Mon Jan 23 15:52:59 IST 2012
4	CLAN-BD	01B02	y	MIN	Y	Mon Jan 23 15:48:59 IST 2012
5	CLAN-BD	01A03	y	MIN	Y	Mon Jan 23 15:48:59 IST 2012
6	CLAN-BD	01A02	y	MIN	Y	Mon Jan 23 15:48:59 IST 2012
7	PKT-INT	01A	n	MIN	Y	Mon Jan 23 15:45:59 IST 2012
8	PKT-BUS	PN 01	n	MIN	Y	Mon Jan 23 15:44:00 IST 2012

Server Alarms

	ID	Source	EvtID	Lvl	Ack	Date	
☐	68	ARB	8	MIN	Y	Mon Jan 23 14:56:04 IST 2012	Both Servers thought they were active

Messaging Alarms

No MESSAGING Alarms

Clear Specific | Clear All | Help

Figure 18: 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.

Filtering alarm report

About this task

You can use the Alarm Report form to filter or sort the Alarm Log. Use this procedure to filter alarm report.

Procedure

1. At the SAT type **`display alarms`** and press `Enter`.

   The Alarm Report form is displayed (the figure on page 116).

```
display alarms                                              Page   1 of   1
                                  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 ):     /
```

Figure 19: Alarm report form

2. Put values in the various fields to display only the alarms that you want:
3. Press `Enter` to submit the form.

   The **Alarm Report** displays. See Communication Manager report interpretation on page 120 to continue diagnosis of the problem.

Alarm report field descriptions

Name	Description
Active	y displays active (unresolved) alarms

Name	Description
	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
Warning	y Displays warning alarms n Omits warning alarms
Interval	h(our) d(ay) w(eek) m(onth) a(ll)
From To	You can use the 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 the Alarm and Error Categories section in Maintenance Commands for Avaya Aura® Communication Manager, Branch Gatewayand Servers (*Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431) for a list of the categories and the maintenance objects included in each.
Extension	Assigned extension number.

Name	Description
Trunk(group/member)	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.

Filtering event report

About this task

You can use the Event Report form to filter or sort the Event Log. Use this procedure to filter event reports.

Procedure

1. At the SAT type **`display events`** and press `Enter`.

   The Event Report form displays.

```
display events                                                Page   1 of   1
                                  EVENT REPORT

      The following options control which events will be displayed.

         EVENT CATEGORY

            Category: vector

         REPORT PERIOD

            Interval: a      From:   /  /  :   To:   /  /  :

         SEARCH OPTIONS

                             Vector Number:
                                Event Type:
                                 Extension:


  IPv6 addresses are truncated, see System Logs web page for complete address
```

   Figure 20: Event report form

2. Put values in the various fields to display only the alarms that you want:
3. Press `Enter` to submit the form.

   The Event Report displays. See Communication Manager report interpretation on page 120 to continue diagnosis of the problem.

Event report field descriptions

Name	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.

Viewing the Web interface logs

Procedure

1. Log in to System Management Interface.
2. Click **Diagnostics** > **System Logs**
   The system displays the System Logs page.
3. In the **Select Log Types** section, select **Communication Manager's hardware error and alarm 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.

The Web interface log entries interpretation on page 120 section describes the various log entry types.

Web interface log entries interpretation

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 system displays alarm information in brackets []. See Communication Manager report interpretation on page 120 to continue diagnosing the problem.

Communication Manager report interpretation

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 Identify the problem on page 105 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.

The figure on page 121 shows an example of a SAT alarm log that illustrates the cause-and-effect relationship between the "first cause" and its consequences.

```
                                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 21: Alarm report (log) from SAT

The figure on page 121 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 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.

Analyzing IP Telephony problem

About this task

Many strategies can identify the location of a IP Telephony problem. For example, one could pinpoint the location of a problem by using the procedure below.

Procedure

1. Analyze protocol layers from the bottom up, starting at the physical layer.
2. First analyze the perceived voice impairments (echo, delay, and voice clipping) if any, and then analyze signaling and network impairment problems.
3. Start with a solution that is most likely to resolve the problem, followed by less likely solutions if necessary.
4. 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.

5. 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.
6. Are compatible codecs used? Review the network region administration for end-to-end compatibility.

Repairing or escalating a problem

About this task

Use this procedure to repair or escalate a problem.

Procedure

1. Investigate more.
2. Check services status for potential service-provider outage.
3. Check status of other telephony and data equipment on same network.
4. Escalate the problem to your technical support representative.
5. If your study of the logs and other status information has clarified the problem and you want to repair the system, see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300430 and *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers (03-300431)*.

Illustrating a repair procedure

About this task

This procedure is an illustration of a repair procedure. Use this procedure as a guide while preforming a repair procedure.

Procedure

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 Filtering alarm report on page 116).

```
                                  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 Filtering alarm report on page 116.

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 for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300430.

   The table on page 124 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 (
   598) failed.(
) below the table tells you what Error Type 1281 means.

   Table 35: ETH-PT Error Log Entries of

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
1281 (598) failed.( )	Any	Station Digital Audit test (#17)	WRN	OFF	**test port | station**

   Error Type 1281 indicates that the terminal is reporting a bad state of health (IP terminal only).

   The table on page 124 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 5141013**) and press Enter.

   The **Test Results** appear.

```
test port S00004
                                  TEST RESULTS
Port        Mtce Name   Alt. Name       Test No.   Result        Error Code
```

```
S00004      DIG-IP-S    5141013         1372        PASS
S00004      DIG-IP-S    40002           1373        FAIL          1007
S00004      DIG-IP-S    5141013         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 for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300430.

   the table shows the Test #1373 Signaling Path PING Test information for Error Code 1007, Test Result of FAIL:

   Table 36: 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. a. Verify that at least one destination is reachable through this port. PING this destination (**`ping ip-address xxx.xxx.xxx.xxx`**). b. If a PING to any destination is successful through this port, the link is up. c. 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. d. If only this station cannot be pinged: • Make sure the personal computer is up. • Make sure the personal computer has a network connection (Ethernet or dial-up). • Check the Ethernet cabling.

7. Perform the repair steps listed in the **Description / Recommendation** column.
8. If the repair steps do not fix the problem, escalate to your technical support representative.

Chapter 5: Troubleshooting IP telephony

TN2302AP IP Media Processor or TN799DP CLAN circuit pack does not work

TN2302AP IP Media Processor or TN799DP CLAN circuit pack does not work because of the causes mentioned below:

- Invalid board location
- No resource administered for a specified region
- Board is not an administered IP-Interface

Inspecting board location

About this task

Use this procedure to check if the entered board location is invalid or does not contain a CLAN (TN799DP) board.

Procedure

Run the **`list configuration`** command to location the TN799DP boards.

Administering a correct resource for a specified region

About this task

Use this procedure to administer a correct resource for a specified region.

Procedure

Enter correct resource type on the IP-Network Region form.

Inspecting administered TN799DP boards

About this task

Use this procedure to check if the entered board location contains a CLAN that has not been administered.

Procedure

Run the **`list ip-interfaces clan`** command to see all administered TN799DP boards.

H.323 trunks troubleshooting

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 **Trunk Group for Channel Selection** field on the H.323 signaling group screen.

In the example shown in the figure on page 129, 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 required. 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 required outcome.

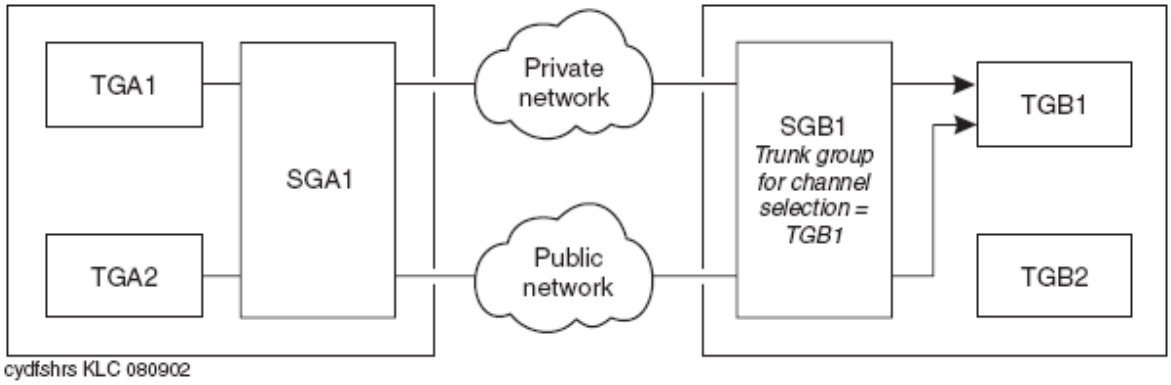


Figure 22: Shared signaling group

The solution to this problem is to set up a separate signaling group for each trunk group, as shown in the figure on page 129. More generally, set up a separate signaling group for each set of trunk groups that have common attributes.

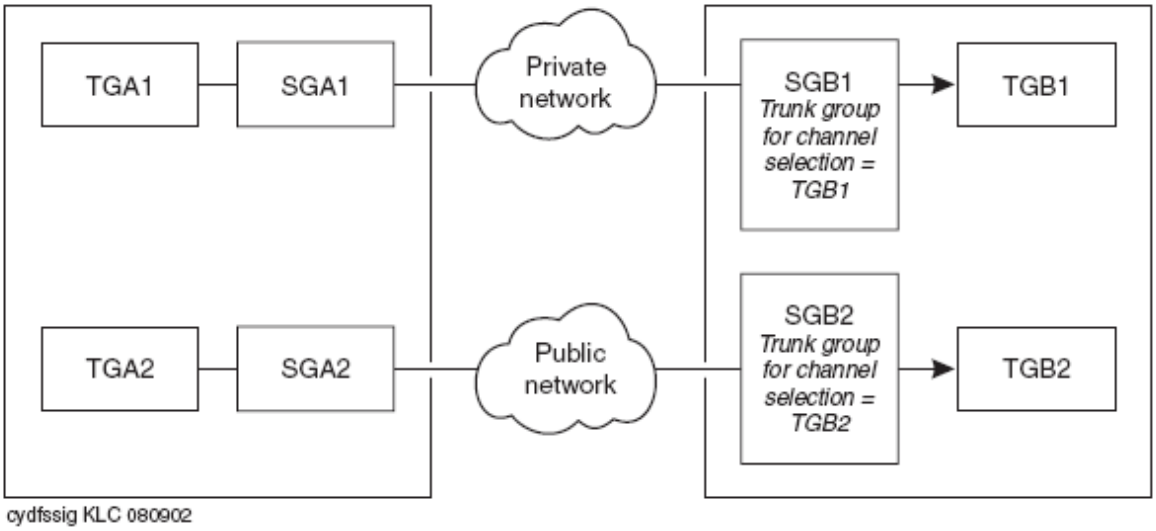


Figure 23: Separate signaling group

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 and you make a call, the call fails even when a second preference is administered in the routing pattern on the source switch. You can use the following procedure to avoid this.

Making a call when no Medpro resources are available

Procedure

Set 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 or WAN segment.

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.

You can use the following procedures to maintain, review, and troubleshoot the status of stations, trunks, and IP network regions:

- Viewing IP connection status of a station
- Viewing IP connection status of a trunk
- Viewing 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 142).

Viewing IP connection status of a station

About this task

Use the status station command to determine the type of active IP connection.

Procedure

1. Type **status station extension** to open the GENERAL STATUS screen.
2. Move to the AUDIO CHANNEL section of the form.

```
status station 5141012                                    Page   x  of   x
AUDIO CHANNEL Port: S00001
              Switch-End Audio Location:
           IP Address                              Port  Node Name      Rgn
Other-End:
  Set-End:
Audio Connection Type: ip-tdm
```

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 go 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.

Viewing IP connection status of a trunk

About this task

Use this procedure to determine the type of active IP connection.

Procedure

1. Type **status trunk group/member** to open the Trunk Status screen.

```
status trunk 0012/001                                     Page   1 of   2
                              TRUNK STATUS
 Trunk Group/Member: 0012/001             Service State: in-service/active
                Port: T00195             Maintenance Busy? no
```

```
 Signaling Group ID: 12
   IGAR Connection? no
    Connected Ports:
status trunk 0012/001                                        Page   2 of   2
                              CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCR
  Signaling   IP Address                              Port
   Near-end:  135.27.152.72                         : 5061
    Far-end:  135.27.153.208                        : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no
 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc:                      Codec Type:
   Audio      IP Address                            Port
   Near-end:
    Far-end:
 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

2. Review the **Audio Connection Type** field using the table in Trunk Status screen field descriptions section.
3. Exit the screen.

Trunk Status field descriptions

Name	Description
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

Name	Description
	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.

Viewing the IP network region status

About this task

You can 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. Use this procedure to determine if any of the IP network regions failed a ping test.

Procedure

1. Type `status ip-network-region x` to open the Inter Network Region Bandwidth Status screen.

```
status ip-network-region 1
               Inter Network Region Bandwidth Status
                                                        Number of     # Times
Src  Dst   Conn    Conn    BW-limits   BW-Used(bits)   Connections   BW-
Limit   IGAR
Rgn  Rgn   Typw    Stat                 Tx      Rx       Tx     Rx Hit
Today  Now/Today
1     2  direct   pass      1 Calls    0       0       0     0      0     0/ 0
1     3  direct   pass      512:kbits  0       0       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 listed on the screen indicate the following:

   - **Dst Rgn**: the regions are not listed; are not administered
   - **fail**: the regions failed the maintenance ping test
   - **pass**: the regions passed the ping test.

3. Exit the screen.

Displaying failed IP network region connections

About this task

You can 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.

Procedure

1. Type **display failed-ip-network-region** to open the first 100 Worst Network Regions report.

```
display failed-ip-network-region
                              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

About this task

You can 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. Use this procedure to test failed IP network regions.

Procedure

1. Type `test failed-ip-network-region #|all` and press `Enter` to begin the test.

   System displays the following Test Results screen at end of the test:

```
                              TEST RESULTS
```

```
Port    Mtce 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.

Considerations for hairpinning and shuffling

This section provides information about hairpinning and shuffling under different circumstances.

- Audio Hairpin Connections come undone: A switch may undo hairpinning of audio connections under following circumstances:
  - A third party is conferenced into the existing two-party call.
  - The switch wants to insert a tone or announcement into the connection.
- Volume is too low 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.
- 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 shuffle, 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.
- 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.

Avaya IP telephones installation or administration is not working

If the Avaya IP telephone installation or administration is not working, try these procedures before contacting your technical support representative for assistance.

Accessing IP Station screens

Procedure

1. Make sure the **IP Stations** field on page 4 of the System Parameters Customer Options screen is set to y.
2. If it is not enabled, you must obtain a new License File.

Viewing virtual LAN port address in the Port field

About this task

Note:

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.

Procedure

Use the **`list registered-ip-stations`** command for a list of registered IP endpoints and their associated ports.

Enabling IP telephone

Procedure

1. Use the **`status station ext#`** command to see if the station is registered.
2. Make sure that in the AUDIO CHANNEL section the **Registration Status** field indicates `registered- authenticated`.
3. To unregister all H.323 endpoints, use the **`reset ip-station`** command.
4. When the SAT displays `Command completed successfully`, it means that the system has started sending reset messages to all of the H.323 endpoints.
5. After sending the reset messages, the system unregisters the endpoint

IP Softphone Troubleshooting

Telecommuter use of telephone lines

The telecommuter application of the IP Softphone requires the use of one telephone line for the IP connection to Communication Manager, which is used for softphone registration and call signaling, and one for a PSTN connection, which Communication Manager uses as a callback number to establish the voice path. How you allocate your telephone lines to these two functions can make a difference.

For example, assume that you have voice mail provided by the local telephone 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

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.

Note:

This information pertains to the RoadWarrior configuration for IP Softphone.

You can access the Avaya Support Web site 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

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.

Diagnosing the no-dial-tone problem

Before you begin

You must check if the network is assessed and modified. If the network is assessed and modified, then there may be a network or MedPro problem. Assuming that multiple IP Telephones are installed, if other IP Telephones experience the same problem there may be a CLAN, a MedPro, or a network problem.

Procedure

1. Verify if the CLAN is operational.

   Refer to Verifying if the CLAN is operational on page 140.

2. If the CLAN board does not show any problem, verify if the MedPro circuit pack is operational.

   Refer to Verifying if the MedPro circuit pack is operational on page 141.

3. If there are no MedPro problems, verify if MedPro is able to ping the IP telephone.

   Refer to Verifying network connectivity between MedPro and the IP telephone on page 142.

4. If IP Telephone is faulty, replace the IP Telephone.

   If MedPro still fails to ping the IP Telephone, go to Step 6. If executing the **`ping ip-address 135.9.42.105 board 07D17`** command has no response, the IP telephone is invisible to the MedPro. Analyze where MedPro ping terminates. Refer to, Analyzing where MedPro ping terminated on page 142.

5. Verify the trasmission speed and transmission duplex (HDX, FDX) compatibility of the MedPro and the Ethernet switch by checking the Layer 1 port statistics on the Ethernet switch connected to the MedPro.

If frame check sequence errors, late collisions, and runts exist, go to Step 7. If not, change the port settings on the Ethernet switch and/or the IP Interfaces form 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 7.

6. Verify the transmission speed and transmission duplex (HDX, FDX) compatibility of the IP Telephone and the Ethernet switch by checking the Layer 1 port statistics on the Ethernet switch connected to the IP Telephone.

   If frame check sequence errors, late collisions, and runts exist, go to Step 8. If not, change the port settings to make speed and mode compatible. If this resolves the problem then no further steps need to be taken.

7. Install a protocol analyzer in the network to capture live traffic and analyze the network in further detail.

   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.

Verifying if the CLAN is operational

About this task

Use this procedure to verify if the CLAN at which the IP telephone is registered is operational.

Procedure

1. Execute the **`status station ext#`** command.
2. 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.

3. 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.
4. 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 for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300430.

5. 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.

Verifying if the MedPro circuit pack is operational

About this task

Use this procedure when there is a problem with many IP Telephones. This procedure can be used to verify if the MedPro circuit pack is operational.

Procedure

1. Go off-hook on the IP telephone.
2. Execute the **status station ext#** command.
3. 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 4; otherwise go to Step 5.
4. There is 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. .
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. If packets are being transmitted normally, go to Step 4.
6. Execute the **list measurements ip dsp-resource** command to determine whether there are sufficient MedPro resources in the system.
7. 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 Software, firmware, and BIOS update on page 284 or the Avaya Support Web site 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.

Verifying network connectivity between MedPro and the IP telephone

About this task

Use this task to verify if MedPro is able to ping the IP telephone.

Procedure

1. Execute the **`status station ext#`** command.
2. 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.
3. Get the IP address of the IP telephone from the **Set-end IP Addr** field.

   Note:

   Hereafter, to simplify the description, it is assumed that this address is 135.9.42.105.
4. Execute the **`ping ip-address 135.9.42.105 board 07D17`** command.
   If MedPro receives echo replies from the IP telephone, there is network connectivity between the MedPro and the IP telephone. If MedPro does not receive the echo reply, the IP Telephone might be faulty.

Analyzing where MedPro ping terminated

About this task

Use this procedure to find out where the MedPro ping terminated from.

Procedure

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 *.”

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 Shuffling and hairpinning on page 130). 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

Dignosing one-way or no-way talk path

Before you begin

For the resolution of this symptom, disable shuffling (if turned on), which forces traffic to use the media processor, and simplifies the analysis of the network. 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.

About this task

Use this procedure to diagnose a one-way or no-way talk path problem.

Procedure

1. If network assessment has been done recently and the network not been modified after the assessment, there may be a network problem, a MedPro problem, or the IP telephone may have outdated software.

   Go to Step 2. If not, 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.

2. If IP Telephones on the same VLAN/subnet/floor experience the same problem, there might be a network problem, or multiple IP Telephones might have outdated firmware.

   If the IP telephone firmware version is outdated, download and install the correct firmware (see Software, firmware, and BIOS update on page 284 or the Avaya Support Web site http://support.avaya.com). If this solves the problem then no further steps are needed, otherwise verify if the call is shuffled. Refer to Verifying if the call is shuffled on page 146.

3. If the call is shuffled, turn off shuffling with the **`change station ext#`** command.

4. 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. Refer to, Verifying if the MedPro can ping the IP Telephones on page 147.

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.

If this does not resolve the problem, then there could be a network problem or a MedPro problem. Although a network problem is still most likely, keep shuffling disabled.

5. Verify if the IP telephone receives a dial-tone.

   If the IP telephone receives a dial tone, verify if there are any Communication Manager errors logged for MedPro or the IP telephone. If the IP telephone does not receive a dial tone, refer to Diagnosing the no-dial-tone problem on page 139 section.

6. Run the **display errors** command to verify if there exist hardware error log and the denial event log for errors against the IP telephone with the particular extension.

7. If the errors exist, use the information in the error log and the *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430 to correct the errors.

   If this solves the problem, no further steps are needed. Otherwise, verify if MedPro receives voice audio from both IP Telephones in the call. Refer to, Verifying if MedPro receives voice audio from both IP Telephones in the call on page 146.

8. If the IP telephone is sending audio, go to Step 5. If the IP telephone is not sending audio or the network is blocking audio packets, exchange the IP telephone.

   If it does not resolve the problem, then there is a network problem that the customer needs to resolve.

9. Verify if the MedPro is operating correctly and has sufficient MedPro audio resources.

   Refer to Verifying if the MedPro operates correctly and has sufficient MedPro audio resources on page 146.

10. If there is a MedPro dynamically allocated to the IP telephone call, go to the Station form (status station ext#) 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 for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430 to resolve the issue. If packets are being transmitted normally, Refer to

Verifying if MedPro receives voice audio from both IP Telephones in the call on page 146.

11. If the AUDIO CHANNEL section on the status station form is blank, this might be because the MedPro cannot allocate resource for the call.
12. Run the **`list measurements ip dsp-resource`** command to determine whether there are sufficient MedPro resources in the system.
13. Check for denials, blockage and out-of-service condition.

    If any of those measurements are greater than 0, this this may indicate that there might exist a problem with the MedPro. Refer to MedPro issues on page 148 for the list of problems that might exist with the MedPro.
14. If there are no MedPro problems, verify if the IP telephone that experiences the 1-way problem or both IP Telephones that experience the no-way problem be pinged from the MedPro.

    Refer to Verifying if the MedPro can ping the IP Telephones on page 147.
15. If the ping is sent, find out the location where the ping terminated by executing 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 21 after the problem has been resolved.
16. Verify if the call traverses through a firewall/ACLs. Refer to Verifying if the call is going through a firewall/ACLs on page 147.
17. If the call traverses, relax the packet/port filtering constraints in the firewall if they are too strict.
18. Check if there are any Layer 1 errors detected in the IP telephone, the intermediate switches/ routers or in the MedPro, by logging into the switches and routers.
19. Check the port statistics.

    Note:

    Some customers will not allow this. In such case, the customer should be requested to provide this information.
20. If the errors exist, there is a network problem (customer responsibility).

    If there are no errors, 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 21 after the problem has been resolved.
21. If needed, return to the original state again by turning shuffling/hairpinning on.

    Refer to Returning to a shuffled state on page 147. However, returning to a shuffled state may bring the problem back. However, returning to a shuffled state may bring the problem back.

Verifying if the call is shuffled

About this task

Use this procedure to verify if the call is shuffled.

Procedure

1. Run the **status station ext#** command if a call is in progress.
2. Scroll to the CALL CONTROL SIGNALLING section and check the option displayed in the **Audio Connection Type** field.
3. If the option displayed is ip-direct, then the call is shuffled.
4. If the **Audio Connection Type** field displays ip-tdm or ip-hairpin, then the call is not shuffled.

Verifying if MedPro receives voice audio from both IP Telephones in the call

About this task

Use this procedure to verify if MedPro receives voice audio from both IP Telephones in the call.

Procedure

1. Execute the **status station ext#** command.
2. Scroll to the NETWORK STATUS section.
3. Look at the **Last Rx/Tx Sequence** field data. These RTP sequence numbers should increase upon repeatedly executing the **status station ext#** command. You may also use Avaya's VoIP Monitoring Manager to verify proper traffic flow.

   If the RTP sequence numbers increase, the IP telephone is sending audio. If the RTP sequence numbers do not increment, the IP telephone is not sending audio or the network is blocking audio packets.

Verifying if the MedPro operates correctly and has sufficient MedPro audio resources

About this task

Use this procedure to verify if the MedPro operates correctly and has sufficient MedPro audio resources.

Procedure

1. Take an IP telephone off-hook.
2. Execute the **status station ext#** command.
3. Scroll to the CALL CONTROL SIGNALLING section.
4. In the AUDIO CHANNEL section if the **Switch Port** field contains a port location then there is a MedPro port that is dynamically allocated to the IP telephone call.

5. 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.

Verifying if the MedPro can ping the IP Telephones

About this task

Use this procedure to verify if the IP telephone that experiences the 1-way problem or both IP Telephones that experience the no-way problem be pinged from the MedPro.

Procedure

1. Run the **status station ext#** command.
2. 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.
3. Obtain the IP address of the IP telephone from the **Set-end IP Addr** field.
4. If the **ping ip-address** *ip address* **board 07D17** command can be executed, the IP Telephones can be pinged from the MedPro.

   If the command is not executed, the IP Telephones cannot be pinged from the MedPro.

Verifying if the call is going through a firewall/ACLs

Procedure

Check if the call would have to traverse a firewall by determining if it is destined to another remote network.

Returning to a shuffled state

About this task

Use this procedure to return to the original state again by turning shuffling/hairpinning on if necessary.

Procedure

1. Run the **change station ext#** command.
2. The **Direct IP-IP Audio Connections** and **IP Audio Hairpinning** fields should be set to y.

MedPro issues

Following is the list of problems that might exist with the MedPro if any of the readings in the denials, blockage, and out-of-service condition columns are greater than 0.

- 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. For more information on updating software, firmware, and BIOS, see Software, firmware, and BIOS update or the Avaya Support Web site 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.

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).

Types of calls

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

Diagnosing poor audio quality problem

Procedure

1. Verify if a network assessment has ever been done and if the network remained unchanged after the assessment.

   If the assessment has been done or if the network remained unchanged, there might be a MedPro, IP telephone or network problem, or the IP telephone might have outdated software. If not, 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. Verify if the other IP Telephones on the same VLAN/subnet/floor experience the same problem.

   If other IP Telephones experience the problem, there may be a network problem, or multiple IP Telephones may have outdated firmware (see Software, firmware, and BIOS update on page 284 or the Avaya Support Web site http://support.avaya.com).

3. Verify if there is a separate VLAN or subnetwork used for voice.

   The customer can check this on the Ethernet switches.

4. If there is a separate VLAN or subnetwork used for voice, check if the Ethernet switch connected to the MedPro is set to auto-negotiation.

5. If there is no separate VLAN or subnetwork used for voice, check if the number of broadcast messages received are lower than 1000 messages per second (this is the number that can safely be handled by the IP telephone).

6. Use the change ip-interface location command to check the ETHERNET OPTIONS settings.

7. If the Auto field is set to y, go to Step 11.

8. If the Auto field is set to n, change the setting to y (auto-negotiation enabled).

   If this is not possible, set the MedPro speed and duplex to match the switch port.

9. Use the network management system or hook up a protocol analyzer to the network to check the number of messages.

   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.

10. If the number of messages are lower than 1000, go to Step 4.

    If not, 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).

11. Verify if the Ethernet switch connected to the IP telephone transmitting in HDX mode by logging 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.

12. If the Ethernet switch is connected, refer to Verifying if 802.1p QoS and IP DiffServ are properly and consistently used in the switches, routers, the MedPro and the CLAN on page 151. If not, 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.

13. Verify if 802.1p QoS and IP DiffServ are properly and consistently used in the switches, routers, the MedPro and the CLAN. Check if the call traverses a WAN link. Refer to Verifying if 802.1p QoS and IP DiffServ are properly and consistently used in the switches, routers, the MedPro and the CLAN on page 151.

14. 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).

15. If the available bandwidth is sufficient, escalate the problem to your technical support representative.

16. Check if the voice codec set to G.729 for calls across a WAN. Refer to, Verifying if the voice codec set to G.729 for calls across a WAN on page 151.

17. If the voice codec is not set to G.729, 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.

18. Check if the end-to-end packet loss less than 1%. Refer to Packet loss analysis tools on page 152. If the loss is less than 1%, 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. If the loss is more than 1%, there might still be a network problem. Escalate the problem to your technical support representative.

Verifying if 802.1p QoS and IP DiffServ are properly and consistently used in the switches, routers, the MedPro and the CLAN

Procedure

1. Check that the QoS usage is consistent by pressing the keypad button sequence `Hold Q O S #` and using 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.
2. In Communication Manager execute **status station ext#** to determine the CLAN circuit pack to which the IP telephone is registered.
3. Run the **display ip-interfaces** command to find the network region for that CLAN circuit pack.
4. Run the **display ip-network-region** command to check the QoS settings for the region.
5. If QoS and IP DiffServ settings in the switches and routers are fine, verify if the voice codec is set to G.729 for calls across a WAN.

   If not, 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.

Verifying if the voice codec set to G.729 for calls across a WAN

Procedure

1. Checked if there is an active call by running the **status station ext#** command.
2. Scroll to the CALL CONTROL SIGNALLING section.

   In the Audio Channel section if it indicates G.729 as the encoder used, the voice codec is set to G.729.

Packet loss analysis tools

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.

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.

Resolving dropped call problems

Procedure

1. Check whether reconnecting the call solves the problem.

   If the call is connected successfully, there may have been an intermittent network problem. No further actions need to be taken unless this happens frequently. If calls are dropped frequently, proceed to step 4.

2. If reconnecting does not resolve the problem, download the latest firmware from http://www.avaya.com/support and install it on your TFTP server (see also Software, firmware, and BIOS update on page 284).

3. To transfer the software to the telephone, type `Hold R E S E T #` on the telephone.

   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 4.

4. Check whether a network assessment has been done and whether the network has been modified after the assessment.

5. If the network assessment has been done and the network has been modified after the assessment, there may be a network problem, a CLAN problem or a MedPro problem. Go to step 1 and explore all possibilities.
6. If a network assessment has not been done, the network may not be compliant with Avaya's network requirements and a (re-) assessment may need to be done. Go to the next step.
7. Check whether other IP telephones experience the same problem.

   If other IP telephones experience the same problem, there may be a network problem, a MedPro problem, or a CLAN problem.
8. 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).
9. 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 6: Troubleshooting trunks

Troubleshooting trunks with Automatic Circuit Assurance

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. An **ACA activate/ deactivate** button (one per system) is required on the telephone or attendant console.

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.

Busy Verification of Terminals and Trunks usage

A multi-appearance telephone or attendant console equipped with a **verify** button is required.

You can use Busy Verification of Terminals and Trunks 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.

ISDN-PRI troubleshooting

The figure on page 156 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.

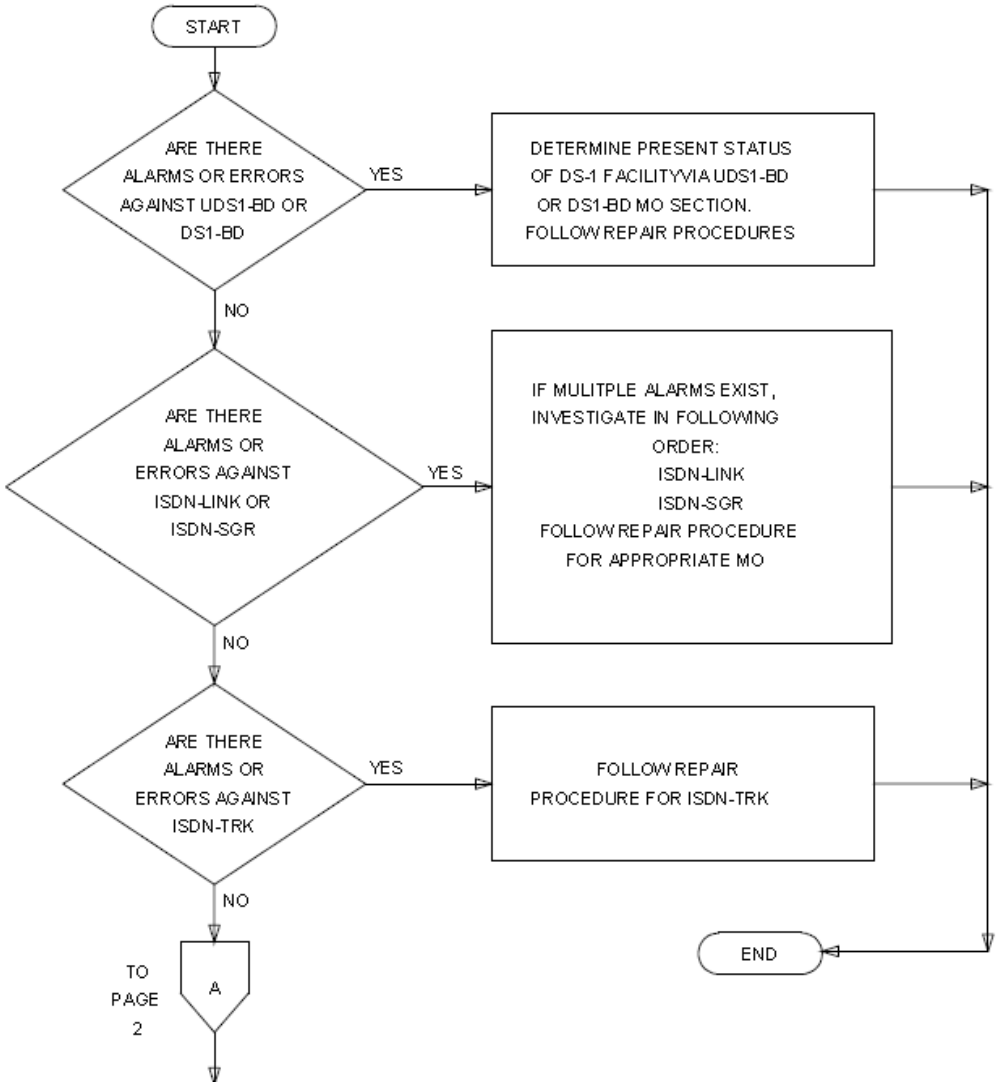


Figure 24: Troubleshooting ISDN-PRI (Page 1 of 2)

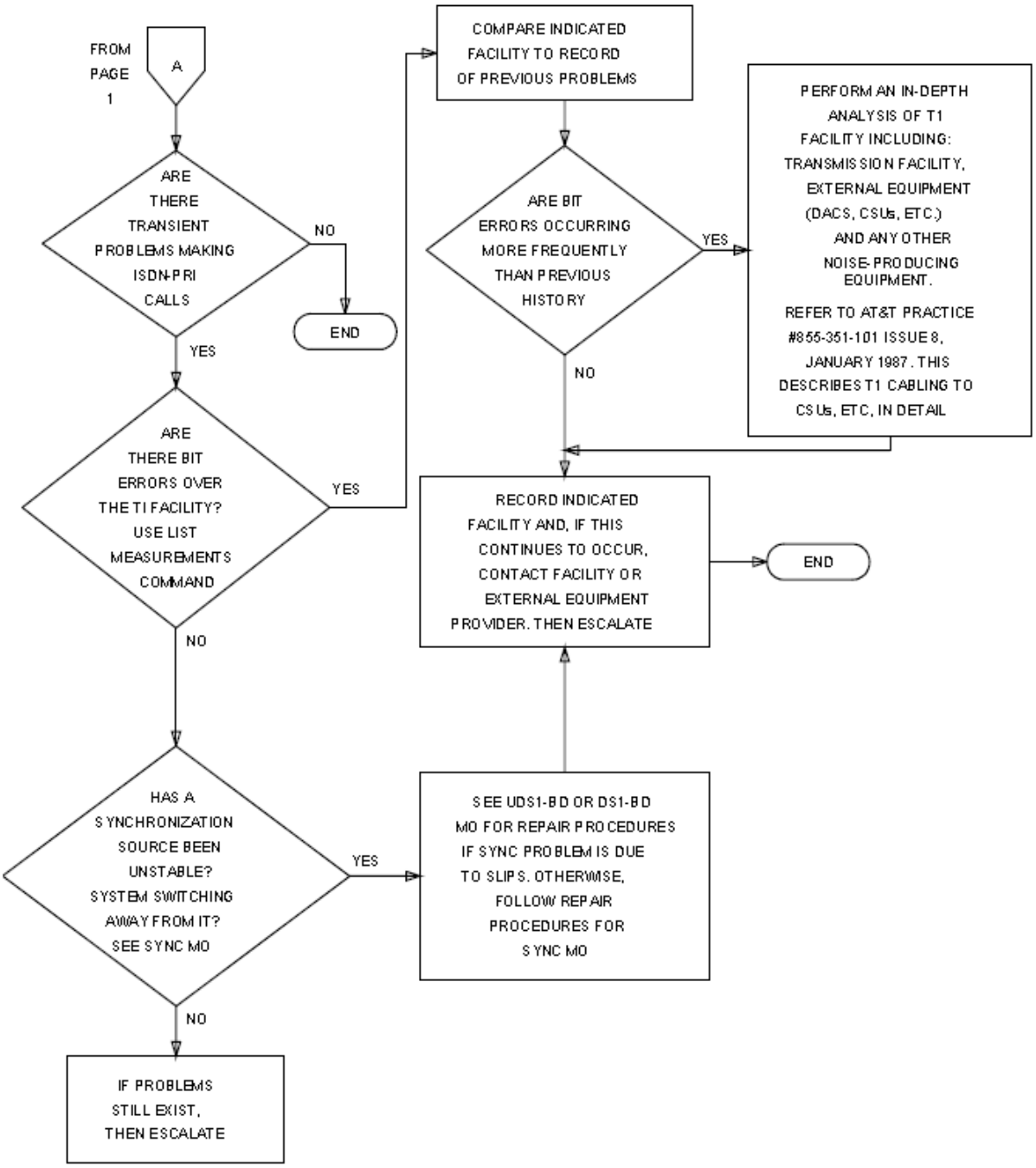


Figure 25: Troubleshooting ISDN-PRI (Page 2 of 2)

Troubleshooting ISDN-PRI endpoints (wideband)

About this task

This procedure 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 layers are investigated in the following order:

- DS1 facility is Layer 1
- TN2312AP IPSI circuit pack's Packet Interface circuit is Layer 2
- PRI endpoint's ports are Layer 3

Note:

This troubleshooting procedure is limited to diagnosing faults between the switch and the ISDN-PRIs. 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.

Procedure

1. If there are alarms or errors against any of the following maintenance objects, resolve those alarms or errors in the order listed at left by following procedures for the appropriate MO in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300430.
   - UDS1-BD
   - PKT-INT
   - SYS-LINK
   - ISDN-LNK
   - ISDN-SGR
   - PE-BCHL
2. If there are no alarms or errors, at the endpoint, check the status of the endpoint equipment or terminal adaptor.
3. If the status of the endpoint equipment or terminal adaptor indicates a problem, follow repair procedures recommended by the provider of the terminal adapter or endpoint equipment.
4. If the administration at the endpoint and on the switch are inconsistent, correct the administration so that both ends match. If both ends already match, check if every call fails, or are the failures transient.

5. If every call 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.
6. Use **list measurements ds1** to check for bit errors over the **DS1** interface between the switch and the terminal adapter or endpoint equipment.
7. If bit errors are confirmed, 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. If the problem is isolated, check for alarms and errors against SYNC.
8. If a synchronization source is stable, or the system does not switch synch sources, follow normal escalation procedure.

ISDN-BRI and ASAI problems

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 26: ISDN-BRI/packet-bus connectivity on page 160 shows the connectivity of the packet bus as it applies to ISDN-BRI signaling.

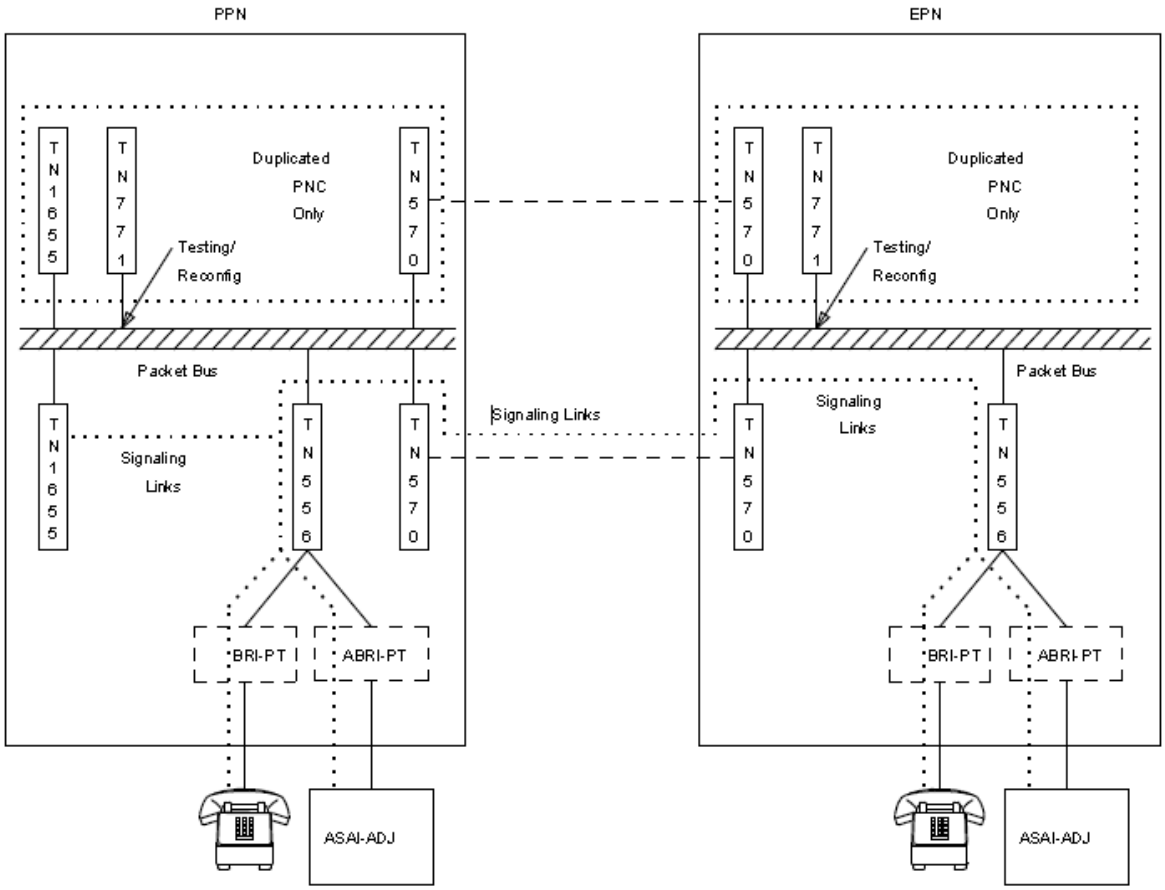


Figure 26: ISDN-BRI/packet-bus connectivity

Flow for troubleshooting ISDN-BRI problems

The flowchart in Figure 27: Troubleshooting ISDN-BRI problems (Page 1 of 2) on page 162 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.

The 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

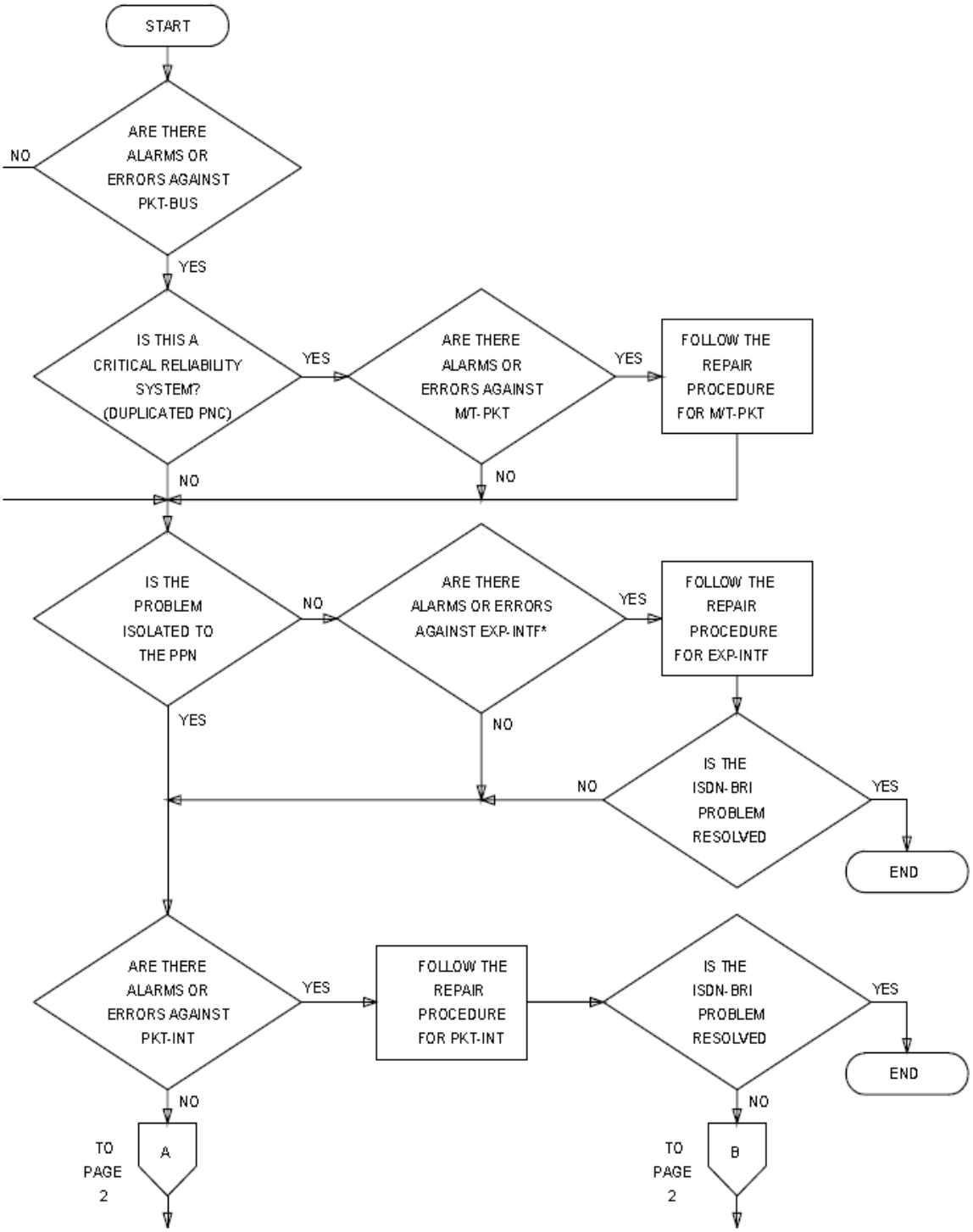
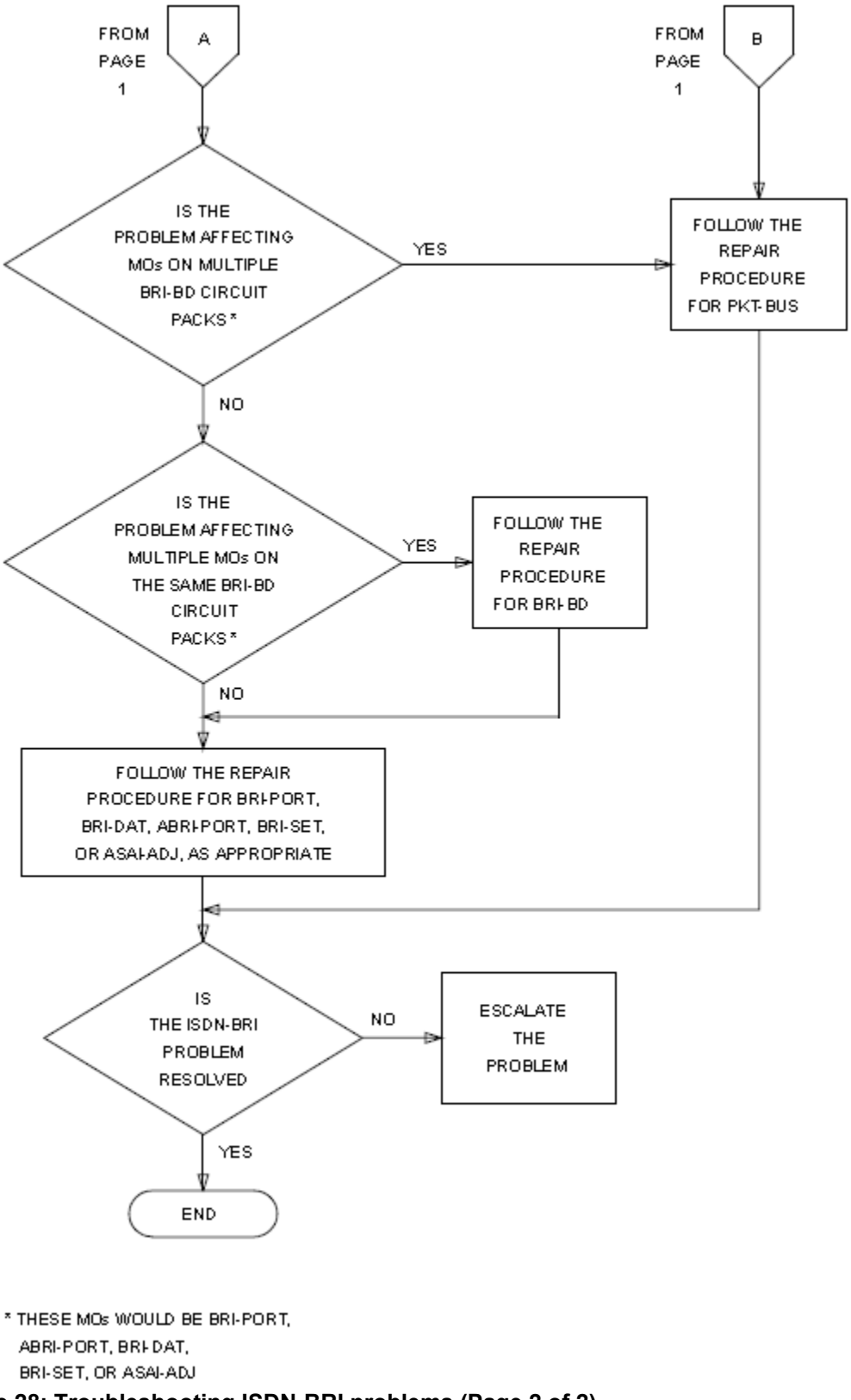


Figure 27: Troubleshooting ISDN-BRI problems (Page 1 of 2)



* THESE MOs WOULD BE BRI-PORT, ABRI-PORT, BRI-DAT, BRI-SET, OR ASAI-ADJ

Figure 28: Troubleshooting ISDN-BRI problems (Page 2 of 2)

Troubleshooting ISDN-BRI and ASAI

Procedure

1. Check whether alarms or errors are present against the packet bus.
   If there are no alarms or errors, go to step 5.
2. Check whether the system is a critical reliability (duplicated PNC) system.
   If the system is not a critical reliability system, go to step 5.
3. Check for alarms or errors against M/T-PKT.
   If there are no alarms or errors against M/T-PKT, go to step 5.
4. Follow the repair procedure for M/T-PKT.
5. Check whether the problem is isolated to the PPN.
   If the problem is not isolated to the PPN, check for alarms or errors against EXP-INTF and follow the repair procedure for EXP-INTF to resolve the problem. When there are no alarms or errors against EXP-INTF, go to step 6.
6. Check for alarms or errors against PKT-INT.
   If there are no alarms or errors against PKT-INT, go to step 10.
7. Follow the repair procedure for PKT-INT.
8. Check whether the ISDN-BRI problem is resolved.
   If the problem is resolved, no further steps are required.
9. If the problem persists, follow the repair procedure for PKT-BUs and go to step 13.
10. Check whether the problem affects MOs on multiple BRI-BD circuit packs.
    If the problem affects multiple MOs on multiple BRI-BD circuit packs, go to step
11. If the problem affects MOs on only one BRI-BD circuit pack, check whether the the problem affects multiple MOs on the same BRI-BD circuit pack.
12. Follow the repair procedure for BRI-PORT, BRI -DAT, ABRI-PORT, BRI-SET, or ASAI-ADJ as appropriate.
13. Check whether the ISDN-BRI problem is resolved.
    If the problem is resolved, the procedure is complete. If not, escalate the problem.

ISDN-PRI test calls troubleshooting

An ISDN-PRI test call is placed across an ISDN-PRI user-network interface to a previously designated number 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 to be able to make the call.

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 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.

The figure on page 166 shows a typical response to the **test isdn-testcall** command:

```
test isdn-testcall

Port    Maintenance Name   Test Number   Test Result  Error Code
1B1501  ISDN-TRK             258           PASS
```

Figure 29: Test ISDN-TestCall response

The functions of the **clear**, **list**, and **status** commands associated with the ISDN Testcall are summarized in Procedure on page 167.

- **clear isdn-testcall**: enables you to cancel an in-progress ISDN-PRI test call and start another test call.
- **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).

Test ISDN-TestCall response field descriptions

Field	Description
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. For more information on ISDN-TRK, see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

Troubleshooting outgoing ISDN-testcall command

Procedure

1. If the Trunk Group screen displays **TestCall BCC** field, 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).

2. 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.
3. 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 made.

Chapter 7: Other troubleshooting

Troubleshooting duplicated servers

The sections, Server initialization and network recovery, 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. Execute the shutdown only when advised by 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.

Spontaneous interchange of a server

If a spontaneous server interchange has occurred, assume that a serious fault has occurred on the current standby server. The occurrence of a recent interchange is displayed in the Bash shell's server screen. 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.

You can 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

Causes of spontaneous interchange of a server

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.

Finding the cause by testing the standby server when the logs do not identify the problem

About this task

Use this procedure to find the cause of spontaneous interchange of a server by testing the standby server when the logs do not identify the problem.

Procedure

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

Isolating fiber link fault

Before you begin

When troubleshooting a critical-reliability system (duplicated port-network connectivity), it is important to 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.

About this task

You can use the following procedure to isolate faults on a fiber link. 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.

Procedure

1. Enter **display alarms** with category pnc.

   Replace the circuit pack(s) if there are any on-board alarms.

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

3. If one or more of the previous errors are present, proceed with Step 9.
4. If not, look for SNI-PEER errors.
5. If there is one SNI circuit pack with many different SNI-PEER error types, replace the indicated SNI circuit pack.

6. 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

7. 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.
8. Exit this procedure.
9. Type `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.
10. Execute **`busyout fiber-link`** *FP*, followed by **`test fiber-link`** *FP* **`long`**.

    If any tests in the sequence fail, proceed with Step 11.

    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.

Running tests for each of the fiber link's endpoints

Procedure

1. **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.
2. If the Board Not Assigned is displayed for an EXP-INTF in a PN, use **test maintenance long** to release an EXP-INTF that may be held reset by a PN's Maintenance circuit pack.
3. If EXP-INTF test (#242) fails, replace the EXP-INTF circuit pack and its lightwave transceiver, and return to Step 10. The EXP-INTF test (#242) runs an on-board loop around if no lightwave transceiver is connected to the EXP-INTF.
4. If SNI test (#757) fails, replace the SNI circuit pack, and return to Step10.
5. If SNI test (#756) fails, replace the SNI circuit pack and its lightwave transceiver, and return to Step 10.
6. If EXP-INTF test (#240) fails, replace the EXP-INTF circuit pack, and return to Step 10.
7. If Test #238 (EXP-INTF) or #989 (SNI) fails, replace the lightwave transceivers and their fiber-optic or metallic cable, and return to Step 10. The faulted component can be further isolated using the Troubleshooting SNI/EI links with manual loop-back on page 175.

   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).]
8. If a DS1 CONV is not administered on the fiber link, follow normal escalation procedures.
9. If a DS1 CONV is administered on the fiber link then check if there is an SNI-BD 513 alarmed error (**display errors**, category = pnc). If the display errors category shows **pnc**, replace cabling between the SNI circuit pack and the DS1C circuit pack.

10. If the alarm persists, replace the DS1C and the SNI circuit packs, and return to Step 10. Else, the connected circuit pack is an EXP-INTF.
11. If Test #238 fails, replace cabling between the EXP-INTF circuit pack and the DS1C circuit pack.
12. If Test #238 continues to fail, replace the DS1C and the EXP-INTF circuit packs, and return to Step 10. Else, **busyout** and **test board** *location* **long** for both DS1C circuit packs, and note every test failure or abort.
13. In a standard-, duplex-, or high-reliability system (nonduplicated PNC), if the test returns `Board not inserted` for either the near-end circuit pack (nearest the server) or far-end circuit pack, replace the cabling between the DS1C circuit pack and the SNI or EXP-INTF circuit pack.
14. Wait 1 minute and retest.
15. 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 10. Else, check if any of the CSU devices are looped back.
16. **Busyout** and **test ds1-facility location external-loop** for each DS1 facility. The tests should fail.
17. 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).
18. If the Test #788 passes and Test #789 fails, at the other end of the DS1C complex, replace the DS1C and its lightwave transceiver (if present). See the figure on page 176 and the figure on page 177. Return to Step 10.
19. If Test #788 and Test #789 fails or aborts, execute **test ds1-facility location long** command for each administered and equipped DS1 facility.
20. If Test #797 fails, run the **test ds1-facility location external-loopback** command for each administered and equipped DS1 facility.
21. 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 the figure on page 177).
22. If Test #799 fails at LB1, the problem is with DS1C #1, CSU #1, or the connections in between.
23. If Test #799 passes at LB1 but fails at LB2, the problem is with CSU #1.
24. 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

About this task

You can 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.

Note:

Do not use this procedure on a connection with a DS1 CONV as an endpoint.

Procedure

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.

Fiber faults with loopback tests isolation

The figure on page 177 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 for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

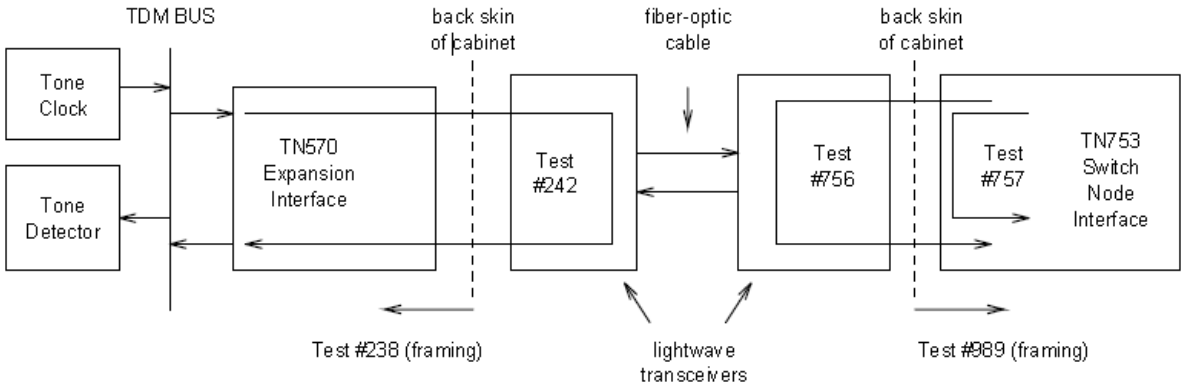


Figure 30: Tests for isolating fiber faults

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 the figure on page 177. For more information about DS1-CONV Loopback Tests (#788 and #789), see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430:

- 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 Loopback Test (#797)
- Near-End External Loopback Test (#799)

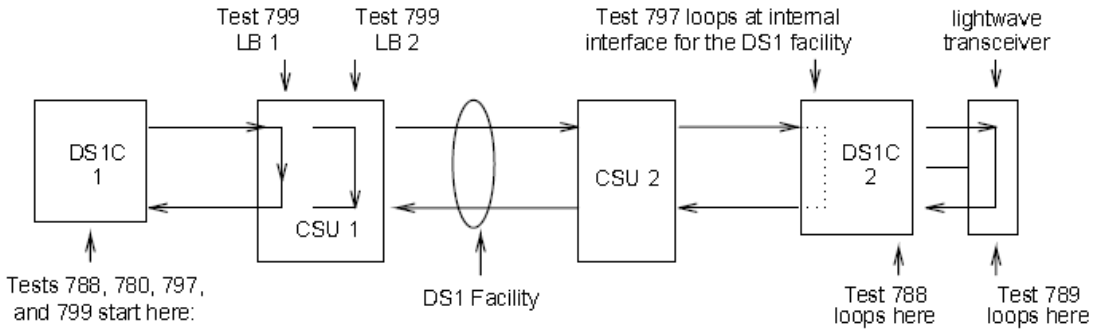


Figure 31: DS1 CONV Loopbacks

DS1 interface cable connectors

The table on page 177 shows the pin assignments for the cable used to connect the TN574 DS1 CONV circuit pack to DS1 facilities.

Table 37: DS1 interface cable connectors

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

Lead	Desig.	50-pin connector pin number	15-pin connector color	Pin	Color
Facility B Line Out	LOB	45	R-BL	09	R-BL
Facility B Line Out	LOB	20	BL-R	01	BL-R
Plug 01					
Facility A Line In	LIA	47	R-O	11	R-O
Facility A Line In	LIA	22	O-R	03	O-R
Facility A Line Out	LOA	48	R-G	09	R-G
Facility A Line Out	LOA	23	G-R	01	G-R

Linux time and Communication Manager time

Linux time is the system time displayed on the Server Date/Time web page or displayed by executing the Linux **date** command. This time is the local time based on the Time Zone selected on the Server Date/Time web page. This is the time used by the system logs and CDR records.

Communication Manager time is the time used by Communication Manager features. If the multilocation feature is not used, this time should be the same as the Linux time. If the multilocation feature is used, the time will depend on the Communication Manager daylight saving rule assigned to a location. Features that used the Communication Manager time based on location include the time-of-day displayed by phones, time-of-day routing for AAR/ARS, and the time-of-day for scheduling Auto Wakeup calls.

Whenever a server's time zone is changed, or whenever a server's daylight saving time rules change, that server must be rebooted.

Troubleshooting problems with Linux time and Communication Manager time

Procedure

1. Check the Server Date/Time web page or run the Linux **date** command. Verify that the Linux time is correct. If the Linux time is correct, go to step 2. Otherwise,
   a. If the incorrect time seems to be related to daylight saving time, check the Release String on the Software Version web page, then check http://support.avaya.com to see if the release needs a patch for daylight saving time.

If a patch for daylight saving time is required, follow the remedial steps provided on the web site.

b. If the system is configured to use a Network Timing Protocol (NTP) time server, verify that the Time Zone setting is correct on the Server Date/Time maintenance web page and refer to Troubleshooting Network Time Server on page 180.

c. If the server is not configured to use an NTP time server, set the system time and Time Zone using the Server Date/Time maintenance web page.

2. Enter the **display daylight-savings rule** SAT command and verify that the start and stop times for Daylight Saving Rule 1 are set correctly.

3. Enter the **display time** SAT command to verify that Daylight Saving Rule is set to 1.

   The default is Daylight Saving Rule 0, but the best practice is to use Daylight Saving Rule 1 so that the Communication Manager daylight saving rule is consistent with the rule used by Linux for the system clock. If the Daylight Saving Rule is set to 0, use the **set time** SAT command to set the Daylight Saving Rule to 1.

4. Enter the **display time** SAT command and verify that the Type is correct (Daylight Saving or Standard).

   If the Type is not correct:

   - Submit the **change daylight-savings-rules** SAT command without changing anything to try to force Communication Manager to think there was a change.
   - You can also change the setting on the **daylight-savings-rules** screen without changing the Linux time to try to force Communication Manager into the right state. For instance, to change the Type to Daylight Saving when it is still set incorrectly to Standard in April, set the stop time to May and the start time to April. Check the **display time** screen to see it the Type gets set correctly, then change the daylight saving rule information back to the correct values.

5. Enter the **display locations** SAT command and verify that the offset and daylight saving rule are correct for the Main location, and, if the multilocation feature is used, verify that the offsets and daylight saving rules are correct for all other locations.

   Daylight Saving Rule 0 should not be used if the multilocation feature is used. (Check for Multi Locations on the system-parameters customer-options screen to see if the feature is used.) The default is Daylight Saving Rule 0, but the best practice is to use Daylight Saving Rule 1, even if the multilocation feature is not used so that the Communication Manager daylight saving rule is consistent with the rule used by Linux for the system clock.

6. Check the Location Codes for cabinets, media-gateways, and ip-network-regions. Check the IP network region assigned on the on **ip-interface** form for C-LANS and the processor interface (procr) for embedded servers in gateways

7. The system must be rebooted if a change was made to the Linux Time Zone setting or if a Daylight Saving Time (DST) patch was applied

Troubleshooting Network Time Server

Procedure

1. Click on **Network Time Sync** under the **Server Configuration** heading (available in Avaya Aura® CM4.0 and later).
2. Check the time specified on the Server Date/Time web page by accessing the web page. If the time is still incorrect, escalate the problem.

Chapter 8: Communication Manager and Linux logs

System intrusion detection

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.

Syslog server

You can administer an external syslog server to receive the data from a number of Communication Manager and Linux logs listed on the System Logs page. In case you do not want to see every log entry for every event, information about how to select the Communication

Manager SAT information that is delivered to the syslog is in Administering logging levels in Communication Manager on page 183. Log entries interpretation on page 198 describes the log format and List of system logs on page 186 describes each individual log along with examples.

Administering the syslog server

About this task

Logging to an external syslog server is disabled by default in Communication Manager. Use this procedure to administer an external syslog server.

Procedure

1. At the System Management Interface (SMI) select **Security** > **Syslog Server** to display the Syslog Server page. Your system might show a different view depending on your configuration.
2. Control File Synchronization of Syslog Configuration gives you the option to synchronize the syslog configuration file with a standby or Survivable Remote Server/Survivable Core Server server:
   - Check **Synchronize syslog configuration to the standby server (duplicated servers)** if you want to synchronize the main server's syslog configuration to the standby server.
   - Check **Synchronize syslog configuration to all LSP and ESS servers** if you want to synchronize the main server's syslog configuration to the administered Survivable Remote Server/Survivable Core Server(s).
3. Click the button next to **Enable logging to the following syslog server**.
4. Type the server name in the **server name** field.

   Note:

   Specify only one server in this field.
5. In the **Select Which Logs Are to be Sent to the Above Server** section, check the boxes next to the names of the logs that you want to send to the external syslog server.
6. Click **Submit**.

Administering logging levels in Communication Manager

About this task

Note:

The defaults in Communication Manager's **Logging Levels** form produce the same amount and type of logging as Communication Manager releases prior to Release 4.0.

In case you do not want all SAT activities logged, you can select the activities to monitor by administering the **Logging Levels** form. Use this procedure to administer logging levels in Communication Manager.

Procedure

1. At the SAT type `change logging-levels` and press `Enter` to display the **Logging Levels** form (the figure on page 183).
2. Administer the fields on page 1.

   To administer the fields, refer to Logging Levels form, page 1 field description table.

```
change logging-levels                                        Page   1 of   2

                                LOGGING LEVELS

 Enable Command Logging? y
        Log Data Values: both

 When enabled, log commands associated with the following actions:

             add? y            export? y                 refresh? y
         busyout? y               get? n                 release? y
  campon-busyout? y                go? y                  remove? y
          cancel? y            import? y                   reset? y
          change? y              list? n                    save? y
           clear? y              mark? y                     set? y
         disable? y           monitor? y                  status? y
         display? n           netstat? y                    test? y
       duplicate? y            notify? y              traceroute? y
          enable? y              ping? y                  upload? y
           erase? y           recycle? y
```

Figure 32: Logging Levels form, page 1

3. Scroll to page two of the **Logging Levels** form (the figure on page 184).
4. Administer the fields on page 2.

   To administer the fields, refer to Logging Levels form, page 2 field description table.

```
change logging-levels                                          Page   2 of   2

                                  LOGGING LEVELS

     Log All Submission Failures: y
         Log PMS/AD Transactions: y
  Log IP Registrations and events: y
     Log CTA/PSA/TTI Transactions: y
```

Figure 33: Logging Levels form, page 2

5. Press `Enter` to submit the form.

Logging Levels form, page 1 field descriptions

Field	Values	Description
Enable Command Logging	no	SAT activity is not logged.
	yes	SAT activity is logged based on the selections on the **Logging Levels** form.
Log Data Values	none	Only the object, the qualifier, and the command action are logged.
	new	Only the new value of any field is logged; the old value is not logged.
	both	Both the field value prior to the change and the field value after the change are logged.
When enabled, log commands associated with the following actions	y(es)	Creates a log entry for this action.
	n(o)	Does not create a log entry for this action.

Logging Levels form, page 2 field descriptions

Field	Values	Description
Log All Submission Failures **Security alert:** Form submission failures due to a security violation are always logged and are not affected by this field.	y(es)	When Communication Manager rejects a form submission for any reason (for example, an invalid entry in a field or a missing value), the event is logged.

Field	Values	Description
	n(o)	When Communication Manager rejects a form submission for any reason, the event is not logged.
Log PMS/AD Transactions	y(es)	Property Management System (PMS) and Abbreviated Dialing (AD) events are logged.
	n(o)	Property Management System (PMS) and Abbreviated Dialing (AD) events are not logged.
Log IP registrations and events	y(es)	IP registrations and IP events are logged
	n(o)	IP registrations and IP events are logged
Log CTA/TTI/PSA Transactions	y(es)	Customer Telephone Activation (CTA), Terminal Translation Initialization (TTI), and Personal Station Access (PSA) events are logged.
	n(o)	Customer Telephone Activation (CTA), Terminal Translation Initialization (TTI), and Personal Station Access (PSA) events are not logged.

Accessing system logs through the Web interface

About this task

Use this procedure to access the system logs through the System Management Interface (SMI) to the Linux server.

Procedure

1. Enter the server IP address in your browser's Address field and press `Enter`.
2. Click **Continue**.
3. At the notification of a secure connection, click **OK**.
4. Click **OK** to accept the security certificate.
   The System Management Interface (SMI) logon page displays.
5. Type your login ID (administered login) in the **Logon ID** field.

Note:

If you are using ASG authentication, start the ASG Soft Key application on your laptop.

6. ASG only: the **Challenge** field is pre-populated; type this number without the hyphens 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 (hyphens permitted in this field) on the Web interface and click on the **Logon** button.
9. Answer Yes to suppressing alarm origination.

   The System Management Interface (SMI) page displays.
10. On the System Management Interface (SMI) page, select **Administration** > **Server (Maintenance)**.
11. In the left-side navigation pane, select **Diagnostics** > **System Logs**.

    The System Logs page displays. Your system might show a different view depending on your configuration.

List of system logs

- Logmanager debug trace
- Operating system boot messages
- Linux scheduled task log (CRON)
- Linux kernel debug messages
- 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 access log
- HTTP/web access log
- Communication Manager Restart log

- Communication Manager file synchronizations
- System update/patch events

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 originated 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 Log entries interpretation on page 198).

Logmanager debug trace

The Logmanager debug trace log lists:

- IP events: use “IPEVT” in the **Match Pattern** field or select the appropriate view (see IP events on page 195 for more information).
- Auto trace-route commands, a subset of the IP Event (IPEVT) entries
- Process entries such as restarts, initializations, shutdowns, duplication status, process errors, system alarms, and communication with external gateways and port networks.

Exporting the log to a separate file

Procedure

1. Select **View** > **Source** in your IE browser menu or right-click in the right pane.
2. Copy and paste to a text processing application.

Operating system boot messages

The Operating system boot messages log lists the boot-up processes from the operating system.

Linux scheduled task log (CRON)

The Linux scheduled task log lists scheduled Linux processes. You can use the Web interface to schedule backups (see *Secure backup procedures* for information about creating scheduled backups.

Note:

Backups and Restores are the only scheduled process that can be initiated from the Web interface.

The figure on page 188 shows two hourly cleanup cycles from a sample Linux CRON log.

```
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)
```

Figure 34: Sample Linux scheduled task log (CRON)

Linux kernel debug messages

Avaya technical service representatives use the Linux kernel debug messages. Linux kernel debug messages contains debug information about the driver, disk, hardware, and memory.

Linux syslog

The Linux syslog lists

- Linux process (system) messages
- Server (Linux platform) errors (in an uninterpreted format)

Note:

For viewing Communication Manager, Linux alarms, and other hardware errors you can use the **Alarms** > **Current Alarms** from the System Management Interface (SMI) for a clearer view of the application and platform alarms. 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 on page 187 log.

- Linux operating system restarts
- Reclaiming a compromised system on page 208 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

The Linux access security 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/web access log on page 194.

- 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 four 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 userlock on page 191.
  - `…failed password check` indicates that the user entered the wrong password.
- Login account is indicated in brackets, for example [craft].
- System originating the request.

```
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
```

Figure 35: Sample log: failed Secure Shell SAT login

What to look for in this log

- Login entries without `successful`are attempts only; you can 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
  ```

- 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)@123.456.789.87], tty[NODEVssh]
  ```

Other considerations

- You cannot set an SNMP trap to monitor login/security violations.

Changing the lockout parameters

Procedure

1. Use the **`userlock`** command to change the login probation interval and login attempts.

   This command is issued at the shell only, not the System Management Interface (SMI).

2. Set up shell access by either logging to the server through the command line interface (CLI), or at the Communication Manager SAT type **go shell** (must have shell access permissions) and press Enter.

userlock

Syntax:

userlock [-u] [-t] [-i] [-o] [-s]

Variable/parameter	Description
-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

The Linux login/logout/reboot log lists:

- Linux logons and logouts
- System reboots

Linux file transfer log

The Linux file transfer log lists:

- Information about files copied to or retrieved from the system, including the time, user, and the filenames involved.

Watchdog logs

The Watchdog 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.

Security alert:

This log does not contain hacking/intrusion information, except for terminating an application.

Platform command history log

The Platform command history 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 log on page 195 view from the System Logs page.

For information about how to read the log entries see Log entries interpretation on page 198.

```
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
```

Figure 36: Sample platform command history log

HTTP/web server error log

The HTTP/web server error 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 the figure on page 193) 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.

```
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
```

Figure 37: Sample HTTP/web error log

What to look for in this log:

- …w_lan_sec2indicates 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&gt;&amp;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

HTTP/Web secure sockets layer (SSL) request log has all the requests made of the Web servers SSL module. HTTP/Web access log indicates all pages requested or placed in non secure mode.

HTTP/web access log

The HTTP web access log lists the activity performed at the Web interface. These are all the requests made of the Web servers SSL module. The SSL request log indicates all pages requested or 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

Communication Manager file synchronizations

Lists the Communication Manager file synchronizations activity.

System update/patch events

Lists the System updates/patches logs.

Select a View

Using the System Logs page, you can 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) log
- 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 SAT events
- Communication Manager’s software events
- Communication Manager’s denial events

IP events

This log lists:

- Interfaces (C-LAN, MEDPRO, VAL, IP stations) up or down
- Registering/unregistering gateways and IP endpoints
- Reason for IP telephone unregistration
- IP address of station registering
- CLAN through which the registration occurred
- Automatic traceroute events

```
20041109:131342365:34112:capro(20388):MED:[ IPEVT    IPT_REG board=01A07 ip= 123.345.567.23
   net_reg=   1  ext=  24100 ip= 123.1345.567.47: 3000 net_reg=   1 reason=normal]
20041109:130224805:34083:capro(20388):MED:[ IPEVT    IPT_REG board=01B07 ip= 123.345.567.21
   net_reg=   1  ext=  24101 ip= 123.345.567.27:49300 net_reg=   1 reason=normal]
20041109:112805025:33726:capro(20388):MED:[ IPEVT  IPT_UNREG board=01A07 ip= 123.345.567.23
   net_reg=   1  ext=  24101 ip= 123.345.567.27:49300 net_reg=   1 reason=2010]
```

Figure 38: Sample IP event log

The final entry in the figure on page 195 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). For more information on denial events, see *Avaya Aura® Communication Manager Denial Events*, 03-602793.

Platform bash command history log

The platform bash command history log lists all commands that have been issued from the server's command line interface (CLI) for the last month.

Some acronyms that appear in this log are:

- PPID = parent process ID
- PID = process ID of shell
- UID = a number that the system associates with a login, for example, "0" is root; all other numbers match to login names.

```
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
```

Figure 39: Sample bash history log

Communication Manager's raw Message Sequence Trace (MST) log

For use by Avaya technical service representatives. If enabled through a SAT command, entries to the Message Sequence Trace (MST) log of Communication Manager can be repeated into the debug trace log in a readable format.

Communication Manager's processed Message Tracer (MDF)

For use by Avaya technical service representatives.

Communication Manager's interpreted Message Tracer (MTA)

The system performs a pre-test to determine if adequate resources are available. If adequate resources are not available, the system displays an error message. You can select the Communication Manager's Message Trace Analyzer (MTA) and Force MTA checkboxes, to override the error and accept the potential consequences.

Communication Manager's hardware error and alarm events

The Communication Manager hardware error and alarm events log lists the same items that report as **`display alarms`** (SAT) or **Alarms** > **Current Alarms** only in log format.

Communication Manager's SAT events

Depending on the Logging Levels, the Communication Manager SAT events log lists the SAT activity according to the administered parameters (see Administering logging levels in Communication Manager on page 183).

Communication Manager's software events

For use by Avaya technical service representatives.

Communication Manager's denial events

The Communication Manager's denial event show the denial events on the system. The denial events are not software errors, but unexpected events caused by mismatched translation, mismatched provisioning, network problems, invalid operation, resource exhaustion.

For more information on denial events, see *Avaya Aura® Communication Manager Denial Events*, 03-602793.

Select Event Range

You can use this section of the **Diagnostics** > **System Logs** page to refine/restrict the log report.

Name	Description
Today	Displays log entries for the current date.
Yesterday	Displays log entries for the previous day.
View entries for this date and time	Specifies 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	Searches for log entries containing the search string that you type into this field.

Display Format

Name	Description
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.
View Log	Generates the log report.

Log entries interpretation

The beginning of each log entry, regardless of log type, has common timestamp information that is detailed in Common timestamp interpretation section. The Platform command history log on page 192 has specific formats and interpretation depending on the application delivering the log information.

Common timestamp interpretation

The beginning of each log entry contains common timestamp information, separated by colons (:), and looks similar to the following:

```
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), an example from the Logmanager debug trace on page 187 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 on page 188 and httperr for the HTTP/web server error log on page 192.
- **MED** is the priority level (medium).

After the common timestamp information, the system displays the log-specific information in brackets []. 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.

Platform bash command history log format

The following general format is used for all log entries in the Platform command history log:

```
mmm dd hh:mm:ss server-name text
```

Table 38: Platform bash command history log format on page 199 lists and describes each field in the command history log.

Table 38: Platform bash command history log format

Name	Description
mmm	The month in text format, for example “Aug”
dd	The day of the month
hh:mm:ss	The time in 24-hour format
server-name	The host name of this server
text	The text field contains the log event text that is supplied by the module logging the event. For more information on the text field see the following sections: • Command history log format for Communication Manager SAT on page 199 • Command history log format for CMS on page 201 • Command history log format for PMS on page 202 • Command history log format for CTA, PSA, and TTI on page 203 • Command history log format for Abbreviated Dialing Button Programming on page 204 • Command history log format for Web activity on page 205

Command history log format for Communication Manager SAT

Depending on the level of logging that is enabled, the format for the text portion of log entries for the Communication Manager SAT is:

```
module-name[pid]: sat sid uid uname profile R action object qualifier
fieldName | oldValue | newValue
```

Table 39: Communication Manager SAT command history log format on page 199 lists and describes the text formats in the log entry for SAT. For more information about logging levels see Administering logging levels in Communication Manager on page 183.

Table 39: Communication Manager SAT command history log format

Command	Description
module-name	The name of the software module that created the entry in the log

Command	Description
pid	The Linux process ID that created the entry in the log
sat	The text string “sat” identifies a Communication Manager SAT log entry.
sid	The parent process ID of the autostat process, or the process ID of the TUI process associated with this SAT session when this SAT session was through a C-LAN.
uid	The SAT user’s numeric ID
uname	The SAT user’s login name
uname2	The SAT user’s secondary login name
profile	The access profile number that is assigned to this user
R	The status of the action: • s: the action was a success • f: the action was a failure other than for a security reason. The letter f could be followed by a colon and an ASCII error code. • v: the action was a failure due to a security violation.
action	The SAT command invoked by the user, for example **add**, **display**, and **list** v
object	The SAT form that was accessed, for example, station, trunk-group, etc.
qualifier	Contains the instance of the form or object. For example, in the **display station 1000** command, the qualifier is “1000.”
fieldName	The name of the field in the SAT form
oldValue	The value of the field before the change
newValue	The value of the field after the change

Examples of SAT log entries

- Commands that do not change data only log the form invocation:

```
module-name[98765]:sat 13533 778 login login 0 s display station 1000
```

This log entry indicates that the user accessed the station form for extension 1000 but did not make any changes.

- One log entry is created for the form invocation and one log entry is created for each field that was changed for commands that change one or more fields within a form:

```
module-name[98765]: sat 13533 778 login login 0 s display station 1000

module-name[98765]: sat 13533 778 login login 0 s change station 1000 Name | Joe
Smith | Mary Jones

module-name[98765]: sat 13533 778 login login 0 s change station 1000 Security
Code | * | *

module-name[98765]: sat 13533 778 login login 0 s change station 1000 Coverage
Path 1 | 3 | 6

module-name[98765]: sat 13533 778 login login 0 s change station 1000
Personalized Ringing Pattern 1 | 2 | 4
```

These entries indicate the following:

- The name associated with extension 1000 changed from Joe Smith to Mary Jones
- The security code for extension 1000 changed, but the security codes (indicated by *) do not display in the log.
- The **Coverage Path 1** field for station 1000 changed from 3 to 6.
- The **Personalized Ringing Pattern 1** field for station 1000 changed from 2 to 4.

Note:

For commands that log new entries, only values that change from a default value are logged.

Security alert:

The values for authorization codes, PINs, encryption keys, and passwords never appear in the command history log.

Command history log format for CMS

Depending on the logging level that is enabled, the format for the text portion of log entries for Call Management System (CMS) is:

```
module-name[pid]: mis uname profile R action object qualifier fieldName |
oldValue | newValue
```

Table 40: CMS command history log format on page 202 lists and describes the text formats in the log entry for CMS. For more information about logging levels see Administering logging levels in Communication Manager on page 183.

Table 40: CMS command history log format

Name	Description
module-name	The name of the software module that created the entry in the log
pid	The Linux process ID that created the entry in the log
mis	The text string “mis” to indicate a CMS-initiated change.
uname	The login name of the CMS user that accessed Communication Manager through CMS. If CMS does not send the uname to Communication Manager, then the uname field contains “na” (not available).
profile	The access profile number assigned to CMS access
action	The command invoked by the user, for example **add**, **display**, and **list**
object	The SAT form that was accessed, for example, station, trunk-group, etc.
qualifier	The instance of the form or object such as station number
fieldName	The name of the field in the SAT form
oldValue	The value of the field before the change
newValue	The value of the field after the change

Command history log format for PMS

Depending on the logging level that is enabled, the format for the text portion of log entries for Property Management System (PMS) is:

```
module-name[pid]: pms R action object qualifier fieldName | oldValue |
newValue
```

Table 41: PMS command history log format on page 203 lists and describes the text formats in the log entry for PMS. For more information about logging levels see Administering logging levels in Communication Manager on page 183.

Table 41: PMS command history log format

Name	Description
module-name	The name of the software module that created the entry in the log
pid	The Linux process ID that created the entry in the log
pms	The text string “pms”
R	The status of the action indicates: • s: the action was a success • f: the action was a failure other than for a security reason. The letter f could be followed by a colon and an ASCII error code. • v: the action was a failure due to a security violation.
action	The command invoked by the user, for example **add**, **display**, and **list**
object	The SAT form that was accessed, for example, station, trunk-group, etc.
qualifier	The instance of the form or object such as station number
fieldName	The name of the field in the SAT form
oldValue	The value of the field before the change
newValue	The value of the field after the change

Command history log format for CTA, PSA, and TTI

The text format for Customer Telephone Activation (CTA), Terminal Translation Initialization (TTI), and Personal Station Access (PSA) log entries is:

```
module-name[pid]: ID R port station
```

Table 42: CTA, PSA, and TTI command history log format on page 203 lists and describes the text formats in the log entry for CTA, PSA, and TTI.

Table 42: CTA, PSA, and TTI command history log format

Name	Description
module-name	The name of the software module that created the entry in the log

Name	Description
pid	The Linux process ID that created the entry in the log
ID	One of the following: • cta: CTA • psa-d: PSA disassociate • psa-a: PSA associate • tti-s: TTI separate • tti-m: TTI merge • ip-a: associate for IP softphone • ip-u: unassociate for IP softphone
R	The status of the action: • s: the action was a success • f: the action was a failure other than for a security reason. The letter f could be followed by a colon and an ASCII error code. • v: the action was a failure due to a security violation.
port	The Communication Manager port identifier, for example, “03A1508”
station	The station extension number

Command history log format for Abbreviated Dialing Button Programming

Depending on the logging level that is enabled, the format for the text portion of log entries for Abbreviated Dialing Button Programming is:

```
module-name[pid]: ad R action object qualifier fieldName | oldValue |
newValue
```

Table 43: Abbreviated Dialing Button Programming command history log format on page 204 lists and describes the text formats in the log entry for Abbreviated Dialing Button Programming. For more information about logging levels see Administering logging levels in Communication Manager on page 183.

Table 43: Abbreviated Dialing Button Programming command history log format

Name	Description
module-name	The name of the software module that created the entry in the log

Name	Description
pid	The Linux process ID that created the entry in the log
ad	The text string “ad” to indicate an Abbreviated Dialing log entry
R	The status of the action: • s: the action was a success • f: the action was a failure other than for a security reason. The letter f could be followed by a colon and an ASCII error code. • v: the action was a failure due to a security violation.
action	The command invoked by the user, for example **add**, **display**, and **list**
object	The SAT form that was accessed, for example, station, trunk-group, etc.
qualifier	The instance of the form or object such as station number
fieldName	The name of the field in the SAT form
oldValue	The value of the field before the change
newValue	The value of the field after the change

Command history log format for Web activity

Depending on the information on a Web page, the text formats for log entries of Web activity are:

```
module-name[pid]: web ip uid uname profile R page-name
```

```
module-name[pid]: web ip uid uname profile R page-name | button | button-name
```

```
module-name[pid]: web ip uid uname profile R page-name | variable-name | value
```

Table 44: Web activity command history log format on page 206 lists and describes the text formats in the log entry for Web activity.

Table 44: Web activity command history log format

Name	Description
module-name	The name of the software module that created the entry in the log
pid	The Linux process ID that created the entry in the log
web	The text string “web” to indicate a web log entry.
ip	The IP address of the user accessing the server
uid	The ID number of the user establishing the Web session
uname	The login name for the user establishing the Web session.
profile	The access profile number assigned to the user
R	The status of the action: • s: the action was a success • f: the action was a failure other than for a security reason. The letter f could be followed by a colon and an ASCII error code. • v: the action was a failure due to a security violation.
page-name	The name of the page that the user accessed
button	The text string “button” to indicate that the next value is the button-name.
button-name	The button label as shown on the form
variable-name	The name of the text box, button, or check box on the form
value	The value of the variable name after the change. In instances where the variable name is the name of a check box, the value is “checked” or “unchecked.”

Creating backup

About this task

Use this task to create web log entries.

Procedure

1. On the Backup Now page, select the **Security File** check box.
2. Select the SCP in the **Method** drop-down list.
   The system displays the Backup Now page.

Log entries without syslog header

The log entries created (without syslog header) are similar to the following:

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | acp xln
| uncheck
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | security
files | check
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | ftp |
check
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | user
name | backupoperator
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | password
| *
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | hostname
| dataserver
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
directory | /cm
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | button
| start backup
```

Only the first event is logged unless the user clicked the **Start Backup** button. Field changes are not logged unless the page is actually submitted. The field name **Avaya Call Processing (ACP) Translations** is abbreviated to try to make the log entry as short as possible, yet still recognizable.

Reclaiming a compromised system

About this task

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.

Use this procedure to reclaim a compromised system.

Procedure

1. Turn off the server and disconnect it from the network.
2. Back up Communication Manager translations, but do not include any system files or system configuration files in the backup.

   For more information, see *Secure backup procedures*. 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).
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 Viewing and restoring backup data files on page 226).
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 9: Secure Backup Procedures

Secure Shell and Secure FTP

The Secure Shell (SSH) and Secure FTP (SFTP) capabilities are highly-secure methods for remote access. Using the administration for this capability, a system administrator can 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.

Applicable platforms or hardware

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

- G430 Branch Gateway
- G450 Branch Gateway
- C350 Multilayer Modular switch
- S8300D, S8510, S8800, HP DL360 G7 or Dell R610 Duplicated Series Server command line
- IBM eserver BladeCenter Type 8677 command line
- Communication Manager System Administration Terminal (SAT) interface on a server using port 5022.

Note:

The client device for remote login must also be enabled and configured for SSH. Refer to the documentation provided with your client personal computer 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 (C-LAN)
- TN2501AP (VAL)

- TN2312AP/BP (IPSI)
- TN2602AP (Crossfire)

SAT commands enable S/FTP sessions through login/password authentication on the C-LAN and VAL circuit packs and SSH on the Crossfire circuit pack. System Management Interface and a Communication Manager command line enable the IPSI session.

Symmetric algorithms

SAT commands enable the C-LAN, 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

The table on page 210 summarizes the hardware, software, Communication Manager releases, commands, and protocols.

Table 45: Comparison of SSH and SFTP capabilities

Circuit pack	Release 3.0		Release 3.1	
	Command[1]	Result	Command[2]	Result
TN799D P(C-LAN)	**enable/ disable filexfr**	Enables/ disables S/FTP	**enable/disable filexfr**	Enables/ disables S/FTP
TN2501A P(VAL)	**enable/ disable filexfr**	Enables/ disables S/FTP	**enable/disable filexfr**	Enables/ disables S/FTP
TN2312A P/ BP(IPSI)	**ipsisession loadipsi**	Enables SSH Enables SFTP	**ipsisession loadipsi**	Enables SSH Enables SFTP

Circuit pack	Release 3.0		Release 3.1	
	Command[1]	Result	Command[2]	Result
TN2602A PCrossfire	**enable session (Secure? = n)**	Enables Telnet (not SSH)	**enable/disable filexfer enable/disable session** [3]	Enables/ disables S/FTP Enables/ disables SSH
[1]Issue commands for C-LAN and VAL from the SAT; issue the **ipsisession** from the IPSI command line interface (CLI). [2]Issue commands for C-LAN and VAL from the SAT; issue the **ipsisession** from the IPSI command line interface (CLI). [3]When moving from secure to insecure sessions or vice-versa, you must disable the established session before attempting the next.				

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.

Reset 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 the table on page 212.

Note:

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

Table 46: Reset dynamic host keys commands

Circuit pack	Command issued from	Command	Permissions
TN799DP(C-LAN)	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

For more information about the commands, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431.

Enabling secure sessions on circuit packs

About this task

This procedure applies only to these circuit packs:

- TN799DP (C-LAN)
- TN2501AP (VAL)
- TN2602AP (Crossfire)

Use this procedure to enable an S/FTP session on a C-LAN or VAL circuit pack.

Procedure

1. At the SAT type **enable filexfr** and press Enter.
   The Enable File Transfer screen displays.

```
enable filexfer  a03                                  Page 1

                                ENABLE FILE TRANSFER

        Login:_______
     Password:_____________
     Password:_____________
       Secure? y
Board Address: _________
```

Figure 40: Enable File Transfer screen

```
enable filexfer  a03                                  Page 1
                                ENABLE FILE TRANSFER
        Login:_______
```

```
     Password:__________
     Password:__________
       Secure? y
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. Submit the form.

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

Disabling secure sessions on circuit packs

About this task

This procedure applies only to these circuit packs:

- TN799DP (C-LAN)
- TN2501AP (VAL)
- TN2602AP (Crossfire)

Use this procedure to disable an S/FTP session on a C-LAN or VAL circuit pack.

Procedure

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

S/FTP is disabled on the circuit pack.

Enabling secure sessions on Crossfire

About this task

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

Use this procedure to enable an S/FTP session on a Crossfire circuit pack.

Procedure

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

   The Enable Session screen displays.

```
enable session                                                Page   1 of   1


                                  ENABLE SESSION

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

Figure 41: Enable Session 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. 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.

Disabling secure sessions on Crossfire

About this task

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

Use this procedure to disable an S/FTP session on a Crossfire circuit pack.

Procedure

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

S/FTP is disabled on the circuit pack.

Secure updates of Avaya software and firmware

You can transfer files to and from the G430/G450 Branch Gateways, and the TN799DP C-LAN circuit pack using Secure Copy (SCP). The primary purpose of SCP for these devices is to securely download Avaya software and firmware updates. Using the SCP alternative, a system administrator can 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:

- S8300D Server
- S8510 Server
- Duplicated Series Server
- G430 Branch Gateway
- G450 Branch Gateway
- TN799DP C-LAN circuit pack

Note:

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

You can use SCP:

- To download firmware to the various media modules on the G430 and G450 Branch Gateways
- With FTP enabled or disabled
- With TFTP enabled or disabled

Enabling or disabling access protocols

About this task

You can use this procedure on the Server Access page to enable or disable access protocols to the server and LAN.

Procedure

1. Log in to the System Management Interface (SMI).
2. In the left-navigation pane, select **Security** > **Server Access**.

The Server Access page displays.

3. Enable or disable services to the server and/or LAN by clicking on the associated buttons.
4. Click **Submit**.

Secure backup procedures for Communication Manager servers

S8510 and Duplicated Series secure backups

Backing up data files for the Avaya S8510 and Duplicated Series Servers

Before you begin

To backup using Secure File Transfer Protocol (SFTP0 or File Transfer Protocol (FTP) or Secure Copy (SCP), keep the following information handy:

- User name
- Password
- Host Name
- Directory (path)

About this task

Use this procedure to create back up data files for the Avaya S8510 and Duplicated Series Servers using the Maintenance Web Pages.

Procedure

1. Log in to the System Management Interface (SMI).
2. From the left side, select **Data Backup/Restore** > **Backup Now**.
   The Backup Now page displays.
3. In the Data Sets section, you can select the data for back up or select the full data backup.
4. In the Specify Data Sets, you can choose the following data subsets:
   - Server and System Files: installation-specific configuration files (for example, 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.
- Avaya Call Processing (ACP) Translations: contains Communication Manager administration: stations, trunks, network regions.
  - Save ACP translations prior to backup: saves translations to the server's hard drive before saving to the media that you will specify in the **Backup Method** section (Step 5 on page 217).
  - Duplicated servers: Select this option when you are backing up the active 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 5 on page 217).

  Duplicated servers: 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.
- Select the Full Backup option to save all the data subsets.

5. In the Backup Method section select the Network Device option. Network Devices backs up the data and stores it on the specified network device.
6. From the **Method** drop-down list you can choose one of the following options:
   - SFTP (Secure File Transfer Protocol) sends backup data to a secured FTP server.
   - 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. FTP must be enabled through the Server Access Web page.
   - SCP (Secure Copy) sets up a SCP session between the server and the network storage device for secure backups.
7. You can use the Encryption option to encrypt the backup data 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.
8. Click **Start Backup** to begin the backup process.

   The Backup Now page displays a progress message indicating that the backup is underway.

9. Duplicated servers: 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.

Backup Method field descriptions

Name	Description
User Name	The user's account name
Password	The user's password
Host Name	The DNS name or IP address of the 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

S8300D Server secure backup procedures

Backing up the Avaya S8300D Server involves two processes:

- Shutting down the Communication Manager Messaging application
- Backing up data files for the Avaya S8300 Server

Shutting down the Communication Manager Messaging application

About this task

Note:

If you are not using the Communication Manager Messaging application, skip to Backing up data files for the Avaya S8300 Server on page 219.

Use this procedure to gather the Communication Manager Messaging data and shutting down the Communication Manager Messaging application.

Procedure

1. To test Communication Manager Messaging 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 Communication Manager Messaging 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 Communication Manager Messaging documentation.
3. In the lower-left corner of your laptop/personal computer, 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 the Communication Manager Messaging application.

   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 voice mail 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 the Communication Manager Messaging application is shut down.

   When the Communication Manager Messaging application is shut down, you will see voice system is down.

Backing up data files for S8300D Server

About this task

Tip:

This backup procedure requires the following information:

- A server IP address
- A directory path
- A user ID and password to access server on the network

Use this procedure for backing up data files for the Avaya S8300D Server using the System Management Interface.

Procedure

1. Log in to the System Management Interface (SMI).
2. In the left-navigation pane, select **Data Backup/Restore** > **Backup Now**.

   The Backup Now page displays.
3. Refer the Backup Now field descriptions table to fill in the required information on the Backup Now page.

   Note:

   Avaya Aura® CM Messaging announcements must be saved in another backup session.

   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.
4. Click **Start Backup** to begin the backup process.

   The Backup Now page displays a progress message indicating that the backup is underway.

Backup Now field descriptions

Name	Description
Data Sets:	
Server and System Files	Installation-specific configuration files (for example, 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.

Name	Description
Avaya Call Processing (ACP) Translations	Contains Communication Manager administration: Stations, trunks, and network regions.
Save ACP translations prior to backup	Saves translations to the server's hard drive before saving to the media that you will specify in the Backup Method section.
Do NOT save ACP translations prior to backup	Translations are saved only to the media that you specify in the Backup Method section.
Backup Method:	
Method	SFTP (Secure File Transfer Protocol) sends backup data to a secured FTP server. FTP (File Transfer Protocol) sends backup data to an FTP server. SCP (Secure Copy) sets up a SCP session between the server and the network storage device for secure backups.
Network Devices	Backs up the data and stores it on the specified network device.
Encryption	Encrypts the backup data through a 15- to 256-character pass phrase (any characters except the following: single quote, backslash, single backquote, quote, and percent)

Viewing backup history

About this task

Use this procedure to view the most recent backups for any server.

Procedure

1. Log in to the System Management Interface (SMI).
2. In the left-navigation pane, select **Data Backup/Restore** > **Backup History**.
   The Backup History page displays.
3. The page lists up to 15 of the most recent backups in reverse chronological order. For example, the first listing is:

   1 sv-gertrude1.111331-20060723.5649

   Interpret the information as follows:

- 1 is the first backup listed.
- sv-gertrude1 is the name of the server.
- 111331 is the time of the backup (11 hours, 13 minutes, 31 seconds or 11:13:31 AM).
- 20060723 is the date of the backup (July 23, 2006).
- 5649 is the process ID (PID), a unique identifier of this backup.

Schedule Backup

Using the Schedule Backup page, you can 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

About this task

Use this procedure to add or change a scheduled backup.

Procedure

1. Log in to the System Management Interface (SMI).
2. From the left side select **Data Backup/Restore** > **Schedule Backup**.
   The Schedule Backup page displays any previously-scheduled backups by type.
3. Choose to
   - Add a new backup to the schedule by clicking **Add**.
   - Change a previously-scheduled backup by clicking the radio button to the left of the backup listed and clicking **Change**.

   The Add New Schedule or Change Current Schedule page displays, respectively. These forms are the same.
4. Refer to the *Add New Schedule field descriptions* table to fill in the appropriate information on the Add New Schedule page.

Note:

Duplicated servers: 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.

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. Select the Day of the Week from the list .
6. 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).
7. Click on either the **Add New Schedule** or the **Change Schedule** button.

   The system verifies the request.

Add New Schedule field descriptions

Name	Description
Data Sets:	
Server and System Files	Contains installation-specific configuration files (for example, server names, IP addresses, and routing information)
Security Files	Contains Avaya Authentication file, logon IDs, passwords or Access Security Gateway (ASG) keys, firewall information, and file monitoring databases.
Avaya Call Processing (ACP) Translations	Contains Communication Manager administration: stations, trunks, network regions, etc.
Save ACP translations prior to backup	Saves translations to the server's hard drive before saving to the media that you will specify in the Backup Method section.
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.

Name	Description
Backup Method:	
Network Device	Backs up the data and stores it on the specified network device
Method:	
Secure File Transfer Protocol (SFTP)	Sends backup data to a secured FTP server.
File Transfer Protocol (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. FTP must be enabled through the Server Access Web page
Secure Copy (SCP)	Sets up a SCP session between the server and the network storage device for secure backups.
Encryption	Encrypts the backup data through a 15- to 256-character pass phrase (any characters except the following: single quote, backslash, single backquote, quote, and percent).
Day of the Week	Displays the occurrence of backup. You can select the once per day option, to take back up once per day. You can select the any/all days of the week option, to take backup on all or any day of the week.

Removing a scheduled backup

About this task

Use this procedure to remove a scheduled backup from the list.

Procedure

1. Log in to the System Management Interface (SMI).
2. From the left side select **Data Backup/Restore** > **Schedule Backup**.
   The Schedule Backup page displays any previously-scheduled backups by type.
3. Click the radio button to the left of the scheduled backup that you want to remove.
4. Click **Remove**.

The system verifies the request.

Viewing backup logs

About this task

Use this procedure to view log of backup images for every backup that has been performed on a server.

Procedure

1. Log in to the System Management Interface (SMI).
2. Select **Data Backup/Restpre** > **Backup Logs**.
   The Backup Logs page displays. For more information about the report refer to Backup logs field descriptions table.
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.
   - Restore: displays detailed information about the backup image.

Backup logs field descriptions

Name	Description
Data Set	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. Server and System Files: contain installation-specific configuration files such as server names, IP addresses, and routing information.

Name	Description
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 and the destination address or path

Viewing and restoring backup data files

About this task

Use this procedure to view or restore Data utility, you can browse, preview, and restore backup data files.

Procedure

1. Log in to the System Management Interface (SMI).
2. From the left side select **Data Backup/Restore** > **View/Restore Data**.
   The View/Restore Data page displays.
3. To view the current contents of a backup, select the source:
   - Network Device: this option requires the following information:
     - Method: Select SCP (Secure Copy) for the greatest security. You can select sftp, ftp, or scp.
   - Local Directory: type the directory path, for example /var/home/ftp/pub.
4. Select the file you want to either preview or restore by clicking the radio button to the left of the file.
5. Click **View**.

Types of backup files

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

Checking backup status

About this task

Use this procedure to display the 15 most recent restores.

Procedure

1. Log in to the System Management Interface (SMI).
2. Select **Data Backup/Restore** > **Restore History**.
   The Restore History page displays.
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 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.

6. The status of the selected backup is displayed. Click **Refresh** to update the list.

Chapter 10: Component replacement

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

About this task

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.

Procedure

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

About this task

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 turning off 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.

Use this procedure to replace the fan power filter.

Procedure

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

About this task

Use this procedure to replace the temperature sensor.

Procedure

1. 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. 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.

Replacing media modules

About this task

Use this procedure to replace media modules in the G450 and G430 gateways. Before replacing any media modules, ensure that you know which are hot-swappable (see Hot swapping media modules on page 47).

Procedure

1. Identify and mark all cables.
2. Remove the cables, making note of the order in which they are removed.
3. Undo the captive screws and slide out the media module currently inserted into the G450 and G430.
4. Position the media module squarely before the selected slot on the front of the G450 and G430 chassis and engage both sides of the module in the interior guides.
5. Slide the module slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengage from the guides.
6. Apply firm pressure to engage the connectors at the back of the chassis.

   The media module connector has different length pins. The long pins engage first to provide grounding. Medium length and short pins provide power and signal.
7. Lock the media module into the chassis by tightening the spring-loaded captive screws on the front of the module.
8. Re-connect the cables in the correct order.

Warning:

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

Server circuit packs reseat and replacement

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 let the maintenance activity proceed. After that, a minor on-board alarm is logged. If the port board is not administered, no alarm is logged.

Warning:

This procedure can be destructive, resulting in a total or partial service outage. Proceed only after consulting and understanding the applicable service documentation for the component. 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.

The table on page 233 lists the circuit packs that require special procedures for reseating and replacing and a link to the specific reseating/replacing information:

Table 47: 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 IPSI circuit pack reuse on page 281.
TN768 TN780 TN2182B	Tone-ClockTone-Clock Tone-Clock for a PN without an IPSI	TONE-BD (Tone-Clock Circuit Pack) (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 (DS1 Converter Circuit Pack)

S8300D Server component maintenance

See *Job Aids for Field Replacement Units for the Avaya S8300D Server with G450 or G430 Branch Gateway* for these procedures:

- Replacing the S8300D Server or the S8300D server hard drive
- Replacing the G450 or G430 branch gateway
- Replacing media and expansion modules

G650 component maintenance

Removing or replacing G650 fan

About this task

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.

Procedure

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 the figure on page 235.
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.

Removing the G650 fan assembly

About this task

The following image helps you to remove the G650 fan assembly.

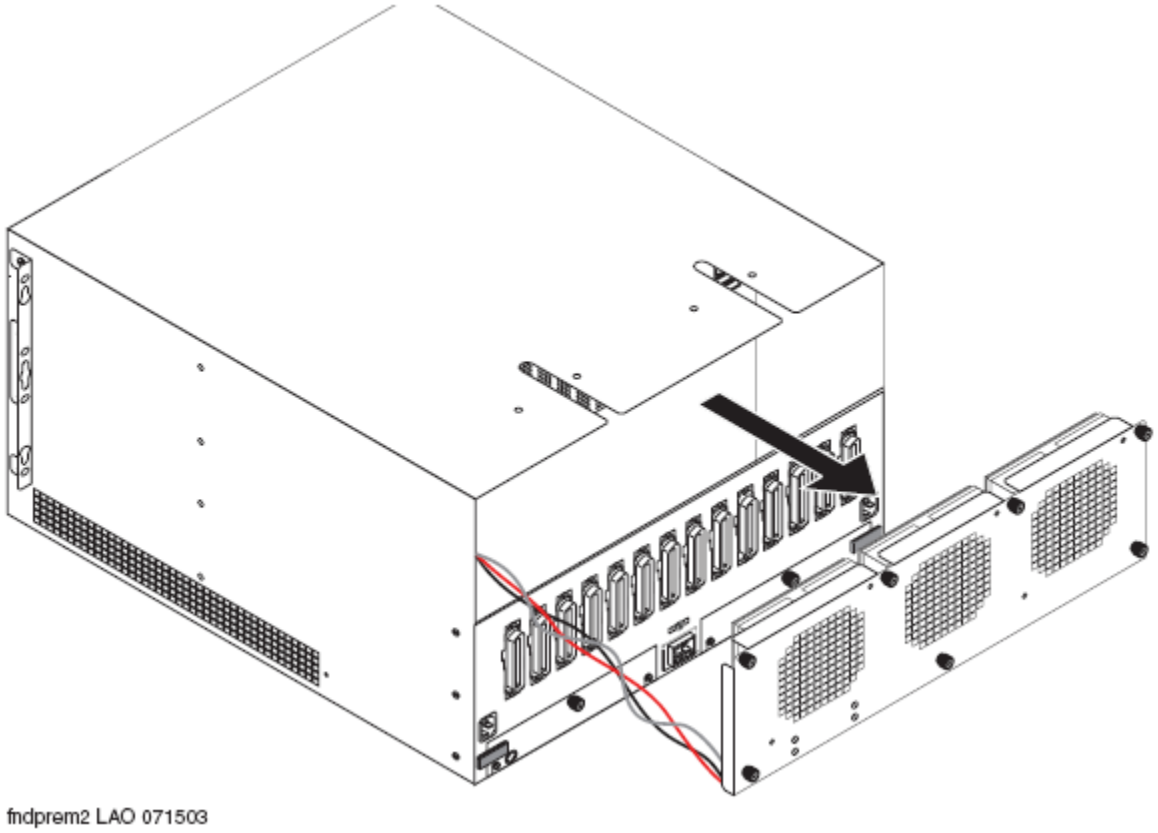


Figure 42: Removing the G650 fan assembly

Replacing a BIU or rectifier

About this task

To remove a battery interface unit (BIU) or rectifier, first attach a grounding strap from the cabinet to your bare wrist, and then perform this procedure.

Procedure

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.

Installing BIU or rectifier

About this task

To install a BIU or rectifier, first attach a grounding strap from the cabinet to your bare wrist, and then perform this procedure.

Procedure

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 11: Packet And Serial Bus Maintenance

Packet-bus faults isolation and repair

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

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) in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.
- A replacement for the TN771D Maintenance/Test circuit pack in the system may be needed. See TN771D stand-alone mode on page 249.
- A backplane pin-replacement kit may be required (see Packet-bus fault correction on page 239). If the kit is not available, replacement of a carrier may be required.

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 241.

Packet-Bus faults

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.

Types of packet-bus faults

Two types of packet-bus faults can occur.

Table 48: Types of packet-bus faults

Type	Description
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 TN754dd 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 fault correction

There are four procedures for correcting packet-bus faults. You can use any of them depending 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 Isolating failures. 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 Isolating failures, 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.

You can follow instructions from either IP-SVR (IP Server Interface) or EXP-INTF (Expansion Interface Circuit Pack) sections to replace the circuit packs.

The packet-bus problem is resolved when all of the following conditions are met:

- Every faulty lead reported by the TN771D's standalone 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.

If the packet-bus problem is present when you insert the circuit pack, but is resolved when you remove the circuit pack, either the circuit pack or the backplane pins in that slot causes the problem. If the backplane pins are intact, you must replace the circuit pack. Keep in mind that there may be more than one failure cause.

In removing and reinserting port circuit packs procedure, 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 standalone mode does not indicate packet-bus faults, perform the removing and reinserting port circuit packs procedure for only the port circuit packs (purple slots) listed in Table 63: Packet circuit packs on page 277 in the detecting circuit pack fault procedure. 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.

Packet bus connectivity

Following maintenance objects communicate on the packet bus.

- 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)

For more information on maintenance objects and tests, see Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300430.

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
- Packet Bus maintenance software
- General fault correction procedures

Packet and TDM buses comparison

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. The packet bus can 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 245).

- 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.

Normal non-packet system traffic can continue unaffected using these interactions, 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. For more information on PKT-BUS (Packet Bus), see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

Correcting general fault

About this task

Use this procedure to isolate the cause and to correct packet bus faults.

Procedure

1. To determine whether a circuit pack that interfaces to the packet bus is the cause of the packet bus problem use the Detecting circuit pack fault procedure.

   This involves examination of the error and alarm logs followed by the usual repair actions.
2. If the packet bus problem persists, you can 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, you can 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, you can replace bus terminators and cables.

   If this does not resolve the problem, you can 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:

- 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:

- TIE-TRK (Analog Tie Trunk)
- DID-TRK (Direct Inward Dial Trunk)
- AUX-TRK (Auxiliary Trunk)

For more information on digital port, analog trunk, and ISDN-PRI trunk testing functions, see Maintenance Alarms for *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

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:

Table 49: LED indicator

LED indicator	Description
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.

LED indicator	Description
	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**. You must 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 standalone mode, these visual indications are still present, but the packet bus is never reconfigured. The amber LED either blinks, or is off.

For more information on TN771D in standalone mode, see TN771D in stand-alone mode on page 248.

TN771D in standalone mode

In TN771D standalone mode, a terminal is connected to the Maintenance/Test circuit pack with an Amphenol connector behind the cabinet. Using this setup, you can perform direct inspection of the packet bus and identify 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 standalone 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 for the TN771D on page 255.
- Terminal or personal computer 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 following cable length:

Table 50: Cable length and Material ID

Cable length	Material ID
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

Selection of a slot for standalone mode

When selecting a slot to use for a TN771D in standalone 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 more information on carrier's power supply units CARR-POW (Carrier Power Supply), see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.
- A slot in a PN's A carrier is preferable if the previous conditions are met.

TN771D standalone 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 standalone mode.

Caution:

A TN771D in standalone mode must be the only TN771D in the PN. If one is already in the PN, place it in standalone 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 standalone

mode causes a loss of service to the packet bus. In this case, this procedure disrupts service.

If standalone mode is entered successfully, the confirmation displays as shown in the figure on page 250.

```
                        TN771 STAND-ALONE MODE

                    (Type "?" at the prompt for help)

Command:
```

Figure 43: Stand-alone mode confirmed

Entering installed TN771D in stand-alone mode for PNs

About this task

Use this procedure to enter already installed TN771D in stand-alone mode for PNs.

Procedure

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.
3. Connect one end of a D8W 8-wire modular cable to port 1 of the 258A.
4. Connect the other end of the cable to a 355A EIA-232 adapter.
5. Plug the EIA-232 adapter into the terminal to be used, and turn the terminal on.
6. 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.

Entering uninstalled TN771D in standalone mode for PNs

About this task

Use this procedure to enter uninstalled TN771D in standalone mode for PNs.

Procedure

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.
2. Connect one end of a D8W 8-wire modular cable to port 1 of the 258A.
3. Connect the other end of the cable to a 355A EIA-232 adapter.
4. Plug the EIA-232 adapter into the terminal to be used, and turn the terminal on.
5. Insert the TN771D circuit pack into the slot.

   The system will not recognize the presence of the circuit pack.

   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. For more information on M/T-BD (Maintenance/Test Circuit Pack) and M/T-PKT (Maintenance/Test Packet Bus Port), see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430. If the TN771D fails while in standalone mode, the message `TN771 circuit pack failed` displays, and no further input is accepted on the terminal. The circuit pack must be replaced.

Exiting standalone mode

About this task

Use this procedure to exit standalone mode.

Procedure

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 standalone mode

When the TN771D is in standalone mode, three commands are available:

Table 51: TN771D stand-alone mode command

Command	Description
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.

The figure on page 252 shows the state of the packet bus leads.

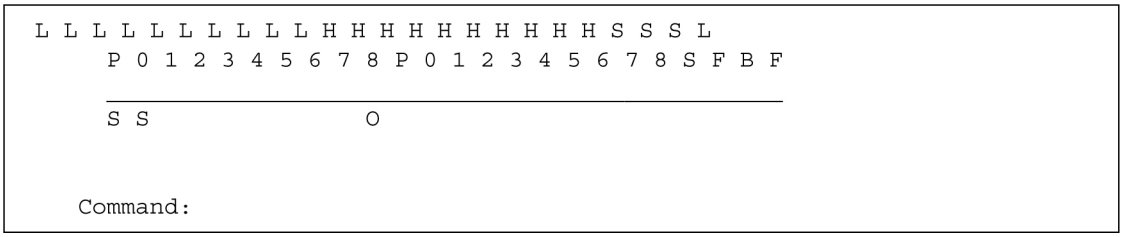


Figure 44: Standalone mode display

- The symbols above the line represent specific leads on the backplane.
- To see the letters and the description, refer to *Standalone mode display field description* table.

Note:

This information is available only from the standalone mode. It is not available from the MT or a remote login.

The figure on page 253 shows the location of the packet bus leads for a given slot as seen from the front and back of the carrier.

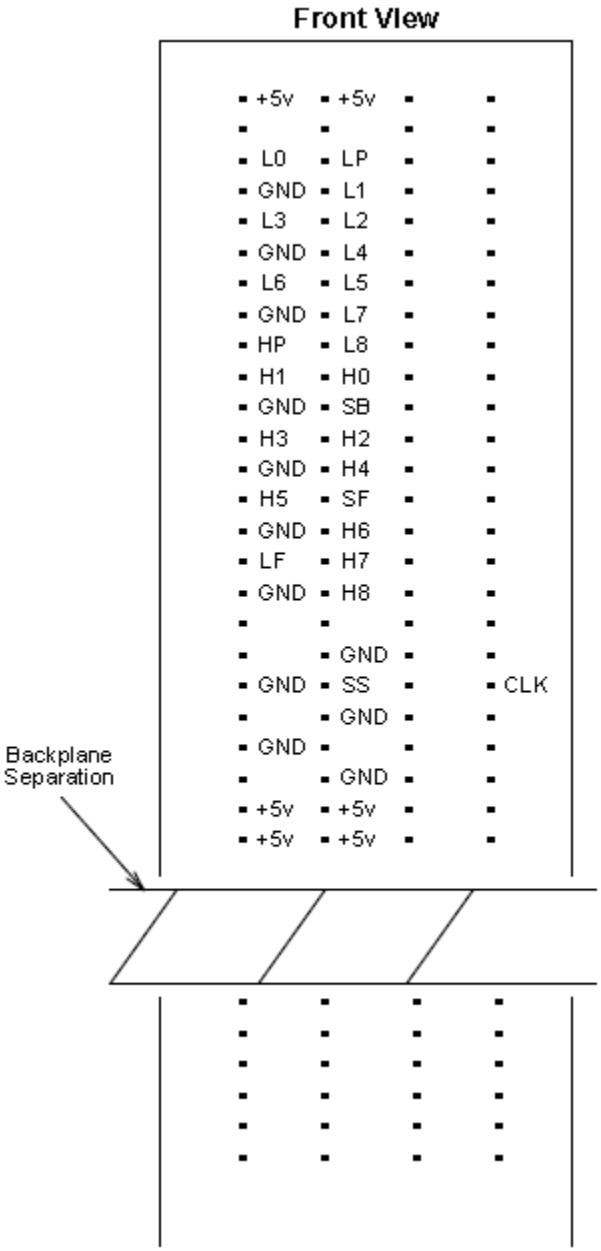


Figure 45: Packet bus leads on the backplane (front view)

The figure on page 254 shows the location of the packet bus leads for a given slot as seen from the front and back of the carrier.

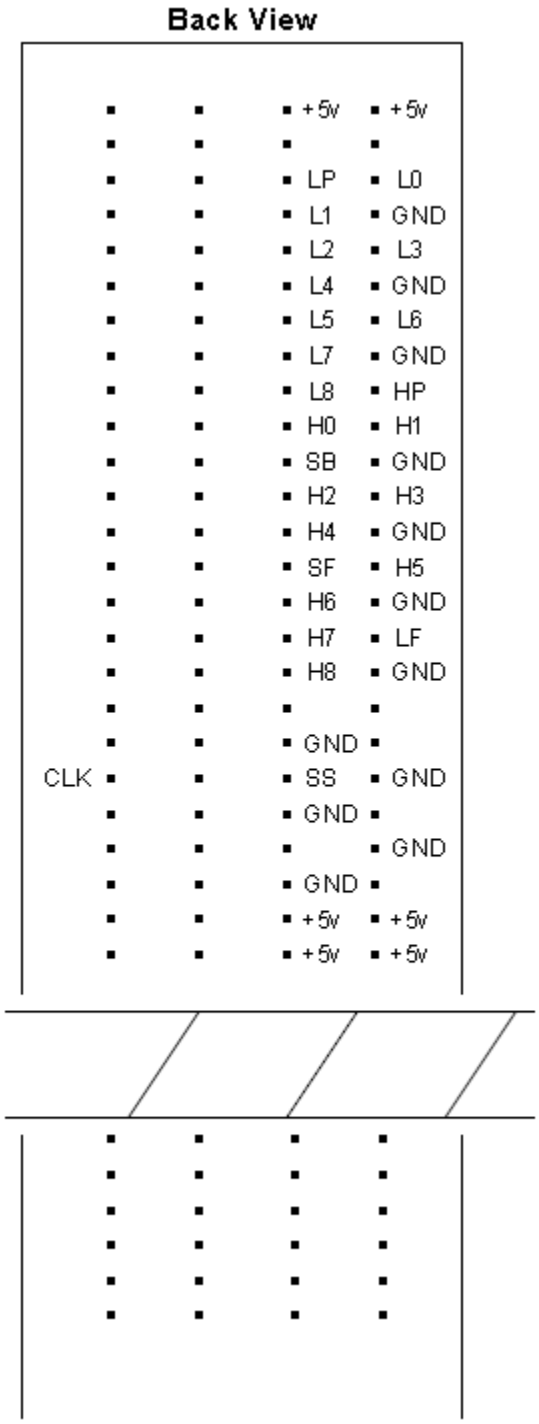


Figure 46: Packet bus leads on the backplane (rear view)

Standalone mode display field descriptions

Name	Description
O	Open lead
S	Shorted lead
blank	No fault

Special precaution for 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.

Analyzing the packet bus problem

About this task

Use this procedure to ensure that the problem is indeed with the packet bus.

Procedure

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

The figure on page 257 and the figure on page 259 show the steps 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.

Table 52: Status commands

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**

Packet bus fault isolation flowchart

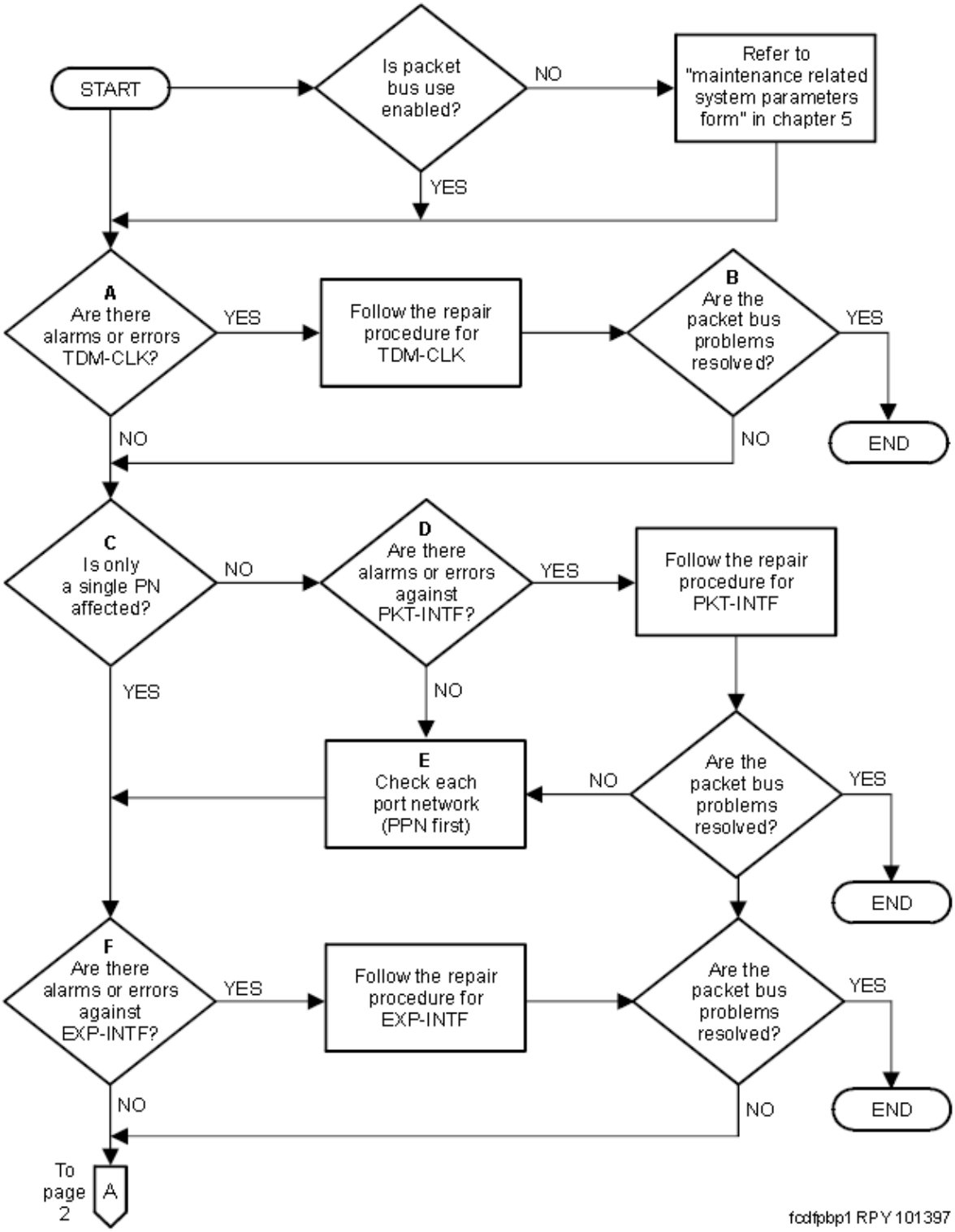


Figure 47: Troubleshooting packet-bus problems (1 of 2)

Note:

Bold-face letters in the flowchart are explained in Flowchart notes on page 260.

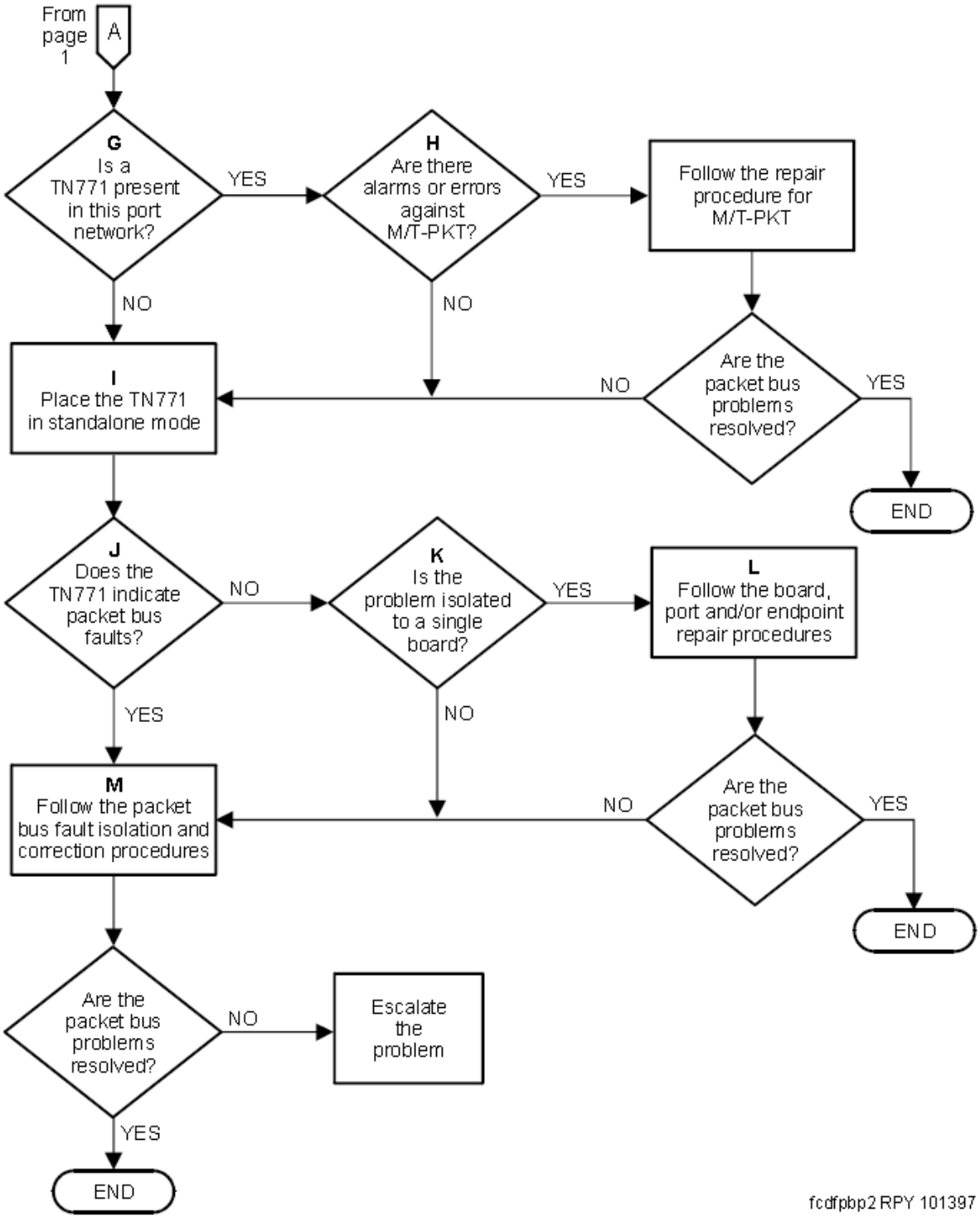


Figure 48: Troubleshooting packet-bus problems (2 of 2)

Note:

Bold-face letters in the flowchart are explained in Flowchart notes on page 260.

Flowchart notes

The following paragraphs refer by letter to corresponding entries in the figure on page 257 and the figure on page 259. 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 standalone mode. See the previous section on standalone 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 standalone 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*. If the packet-bus problem cannot be resolved with these procedures, follow normal escalation procedures.

Packet-bus faults correction

The **`Status port-network P`** command displays 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, Communication Manager Messaging, 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 for the TN771D on page 255.

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. To ensure that a -5 Volt power supply is available, see CARR-POW (Carrier Power Supply).

Considerations for duplicated systems only

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).

For more information on PKT-INT (Packet Interface), EXP-INTF (Expansion Interface Circuit Pack), and TDM-CLK (TDM Bus Clock), see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

Troubleshooting procedures

Detecting circuit pack fault

About this task

Use this procedure to determine whether any circuit packs that use the packet bus have faults. For each circuit pack type in the table on page 263 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.

Procedure

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, no further action is required.
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 *Removing and reinserting port circuit packs*.

Table 53: Packet circuit packs

Circuit Pack Name	Code	Associated maintenance objects
ISDN-BRI	TN556	BRI-BDBRI-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

Removing and reinserting port circuit packs

About this task

Use this procedure to remove and reinsert port circuit packs (purple slots) and the EI circuit pack one or several at a time. You can use this procedure 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 PN's control circuit packs removal and reinsertion for the TN768, TN780, or TN2182 Tone-Clock circuit pack in a high- or critical-reliability system.

Procedure

1. Remove one or several circuit packs.
2. Determine whether the packet-bus fault is still present. If not, go to Step 4.
3. If the packet-bus fault is still present, determine whether the backplane pins in the removed circuit pack's slot are bent using the output from the Maintenance/Test circuit pack's standalone mode and the backplane illustrations that appear earlier in this discussion.
   - If the backplane pins are bent:
     - Turn off 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, perform the following steps:

- 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.

PN’s control circuit packs removal and reinsertion

You can remove and reinsert 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.

Repairing packet bus faults in simplex control circuit packs

Procedure

1. Turn off 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 on and let 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, no further steps are required.

7. If the problem is still present, continue:

   a. If the old circuit pack was reinserted in Step 5 on page 266, replace the circuit pack, and repeat Procedure 3.
   b. If the circuit pack was replaced in Step 5 on page 266, repeat PN's control circuit packs removal and reinsertion for the next simplex control circuit pack.

Result

If PN's control circuit packs removal and reinsertion fails to identify the cause of the problem, go to Isolating failure.

Configuring high- and critical-reliability systems

Procedure

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. Turn off 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 on page 266, replace the circuit pack, and repeat Procedure 3 starting at Step 2 on page 266.
b. If the circuit pack was replaced with a new one, proceed with Step 6 on page 267.

6. Repeat this procedure for the other Tone-Clock. If both have already been checked, continue with Step 7 on page 267.
7. If every PN control circuit pack has been checked and the problem is still not resolved, continue with *Isolating failures*.

Isolating failures

About this task

You can use this procedure 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. Isolating failures is done in two parts. Isolating failures part 1 attempts to clear the packet-bus fault by replacing every bus cable and terminator within a PN. Isolating failures part 2 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.

Procedure

1. Replace the TDM/LAN cable assemblies and TDM/LAN terminating resistors.
2. If this action does not resolve the packet-bus fault, configure the carriers by moving the terminating resistors on the carrier backplanes in such a manner that certain carriers are disconnected from the bus.
3. 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 Carrier rewiring example—rear view of G650 gateway on page 268).
4. Once the length of the packet bus is modified with this procedure, keep the circuit packs that are essential to system operation (and the TN771D Maintenance/Test circuit pack in standalone mode) connected to the new shortened packet and TDM buses.

Note:

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.

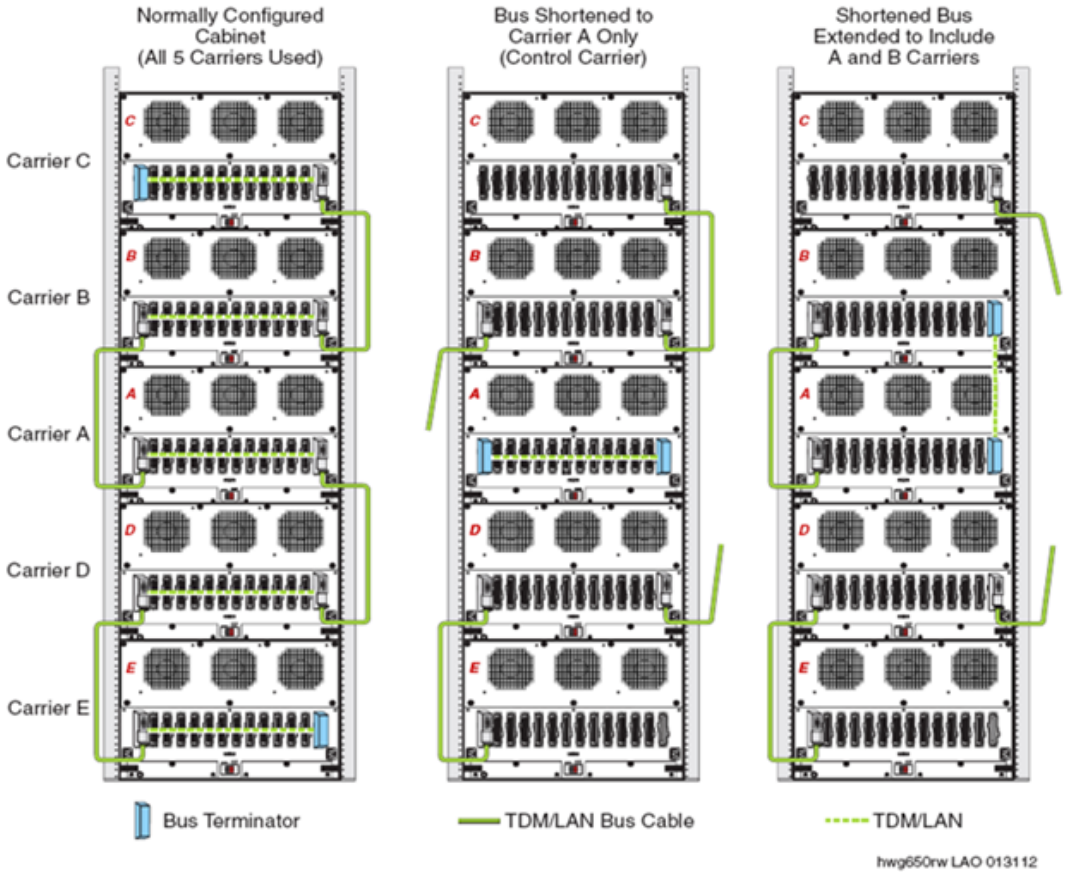


Figure 49: Carrier rewiring example—rear view of G650 gateway

Clearing the packet bus fault

About this task

Use this procedure to clear the packet-bus fault by replacing every bus cable and terminator within a PN.

Procedure

1. Turn off 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 Isolating fault to a particular carrier on page 269.

Isolating fault to a particular carrier

About this task

Use this procedure to isolate the fault to a particular carrier by extending the packet bus from the control carrier to additional carriers one at a time.

Procedure

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. Turn off 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 the Removing and reinserting port circuit packs procedure and/or refer to PN's control circuit packs removal and reinsertion, 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 the Removing and reinserting port circuit packs procedure and/or refer to PN's control circuit packs removal and reinsertion, 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, the Removing and reinserting port circuit packs procedure or PN's control circuit packs removal and reinsertion do not resolve the problem, the added carrier 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. Using this serial bus, the IPSI-2 (TN2312BP) can 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.

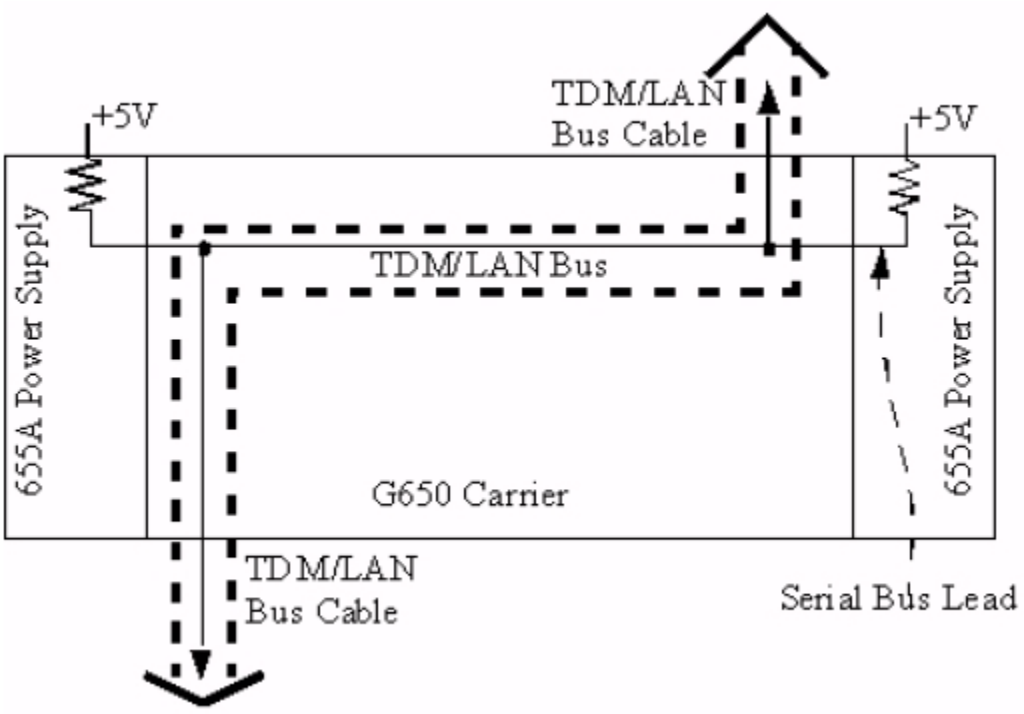


Figure 50: TDM/LAN bus connection to the Serial Bus

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 does not 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:

- You must 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.
- You must 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.

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, you can 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 the Removing and reinserting port circuit packs procedure 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 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.

Removing and reinserting port circuit packs one or more at a time

About this task

Use this procedure to remove and reinsert port circuit packs (those in the purple slots) one or more at a time. You can repeat 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.

Procedure

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 on page 272, 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.

Serial Bus failure isolation

Serial bus failure isolation attempts to isolate the Serial Bus failure to a particular set of carriers. Only the circuit packs in selected carriers are checked. You can use the information in this section if the Removing and reinserting port circuit packs one or more at a time procedure 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.

Serial Bus failure isolation is organized into two parts:

- Replacing all bus cabling and terminators: attempts to clear the Serial Bus fault by replacing all the bus cabling and terminators within a port-network.
- Isolating fault to a particular carrier: 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.

Terminating a Serial Bus at the end of a particular carrier

About this task

Use this procedure to terminate a serial bus at the end of a particular carrier.

Procedure

1. Unplug the Serial Bus cable that connects the carrier to the next carrier and replace with the TDM/LAN Bus terminator.
2. When the length of the Serial Bus is modified, keep the A carrier IPSI-2 circuit pack that is essential to the Serial Bus operation and Serial Bus maintenance connected to the new, shortened Serial Bus.
3. After making and verifying the cabling changes, restore power to the port network.

   Do not insert the Circuit packs in carriers that are not part of the shortened bus. These circuit packs are alarmed.
4. Ignore these alarms for now. Resolve all the alarms when the cabinet is restored to its original configuration.

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.

Replacing all bus cabling and terminators

About this task

Use this procedure to replace all bus cabling and terminators.

Procedure

1. If spare TDM/LAN cable assemblies and TDM/LAN Bus Terminators are not available, go to the isolating fault to a particular carrier procedure.
2. Turn off 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 the Isolating fault to a particular carrier procedure.

Isolating fault to a particular carrier

About this task

Use this procedure to isolate the fault to a particular carrier.

Procedure

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 12: Additional maintenance procedures

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.

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 277.

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 54: 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

SBS Originating Node		
Command	**Shows Connected Ports**	**Shows SBS Associated Port**
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 278 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 55: Error Conditions

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

Error Condition	Cause Value	LAR or non-LAR	Tone Treatment	Software Error or Denial Event
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
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

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

About this task

Use this procedure to find assigned SBS extensions.

Procedure

1. Type `list stations type sbs` and press `Enter`.

   The system displays the Stations form (the figure on page 280) that shows the administered SBS extensions.

2. Press `Enter` to save the 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
```

Figure 51: Stations screen

IPSI circuit pack reuse

If you are reusing 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 on page 281
- Moving from static to dynamic addressing on page 284
- 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

About this task

Use this procedure to change a TN2312AP/BP IPSI from a DHCP address configuration to a static IP address configuration.

Procedure

1. Plug the circuit pack into the appropriate slot in the gateway or if already plugged in, reseat it (unplug and replug).
2. 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**.
3. Telnet to the IPSI using **`telnet 192.11.13.6`**.
4. At the IPSI prompt, enter **`ipsilogin`** to log in to the IPSI IP Admin Utility.
5. Log in using **craft** and the IPSI password.
6. Type **`set control interface ipaddr netmask`** and press `Enter`.
7. If required, set the gateway IP address (**`set control gateway gateway`**, where gateway is the IP customer-provided IP address for their gateway).
8. 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.

9. Telnet to 192.11.13.6 and login.
10. If a default gateway is used, enter the gateway IP address using **set control gateway gatewayaddr**.
11. Enter **quit** to save the changes and exit the IPSI session.
12. Telnet to 192.11.13.6 and login.
13. Use **show control interface** to verify the administration.
14. Enter **quit** exit the IPSI session.

Setting the VLAN and diffserv parameters

About this task

Use this procedure if required, to set the VLAN and diffserv parameters.

Procedure

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.

Resetting the IPSI and exit the IPSI IP Admin Utility

About this task

Use this procedure to reset the IPSI and exit the IPSI IP admin utility.

Procedure

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.

Verifying the IPSI translations

About this task

After all of the IPSIs have been administered, verify IPSI translations and connectivity.

Procedure

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 System Management Interface (SMI) 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

About this task

Use this procedure to change a TN2312AP/BP IPSI from a static IP address configuration to a DHCP (dynamic) address configuration.

Procedure

1. Plug the circuit pack into the appropriate slot in the 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.

Software, firmware, and BIOS update

Use the information sources listed in the following table to update software, firmware, or BIOS on Avaya equipment.

Table 56: Update information sources

Equipment	Information source
TN circuit packs	• FW-DWNLD (Firmware Download) in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430. • Lists of available firmware and a compatibility matrix is located at Avaya Support website at http://support.avaya.com/. Select **Downloads** > **Communication Manager**
S8510 Server	*Job Aids for Upgrading Firmware on the BIOS—Avaya S8510 Server* • Upgrading firmware on the IPSIs • Upgrading firmware on the Avaya Ethernet switch • Upgrading firmware on the maintenance adapter • Upgrading firmware on the BIOS

Equipment	Information source
	For Remote Supervisor Adapter information, see Avaya RSA Users' Guide.
Duplicated Servers	*Upgrading Avaya Aura® Communication Manager, 03-603560 Converting Avaya Servers and Gateways*, 03-602884 • Upgrading firmware on the IPSIs • Upgrading firmware on the Avaya Ethernet switch
4600 Series Telephones 96xx Series Deskphones	For information on FW-STDL (Firmware Station Download), see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

DS1 span testing with a loopback jack

The DS1 Customer Premises Equipment (CPE) loopback jack is a hardware device that loops the CPE's transmitted DS1 signal back to the CPE's receive DS1 signal to test and isolate potential wiring faults in the DS1 span between the system and the network interface point. The loopback jack is used with the following DS1 interfaces:

- TN767D (or later)
- TN464F (or later)
- MM710
- TIM510
- G250-DS1

The DS1 line can be either private or through a DS1 service provider. The interface to the DS1 line can be either a direct interface to a repeatered line or through a Smart Jack that is typically provided at the network interface. The loopback jack works in configurations that use

- no Channel Service Unit (CSU)
- an external CSU
- a CSU module between the DS1 interface and the interface to the DS1 line

Note:

The loopback jack operates with the 120A 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.

- If there is no extended demarcation point, install the loopback jack directly at the network interface point as shown in the figure on page 293.
- If there is an extended demarcation point and the Smart Jack is not accessible, install the loopback jack as shown in the figure on page 294.
- If there is an extended demarcation point, but the Smart Jack is accessible, install the loopback jack as shown in the figure on page 295.

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 the figure on page 297 and the figure on page 298.

Installing loopback jack

About this task

Use this procedure to install the loopback jack.

Procedure

1. Disconnect the RJ-48 (8-wide) connector at the appropriate interface point and connect the loopback jack in series with the DS1 span. See the figure on page 293 through the figure on page 298.
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.

Administering loopback jack

About this task

Use this procedure to administer the loopback jack.

Procedure

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. Using this loopback jack, a technician can determine that the facility is available for remote testing.
4. Enter **`save translation`** to save the changes.

DS1 span tests

This test should only be performed after the DS1 circuit pack and the 120A 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 needed.

Testing the DS1 span

Procedure

1. Enter **busyout board location** to busy out the DS1 circuit pack.
2. At the SAT terminal, enter `change ds1` *location* and verify that 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.
4. Press `Enter` to save the changes.
5. Enter **test ds1-loop** *location* **cpe-loopback-jack**.

   This command 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.
6. Enter **clear meas ds1 loop location** to clear the bit error count.
7. Enter **clear meas ds1 log location** to clear the performance measurement counts.
8. Enter **clear meas ds1 esf location** to clear the ESF error count.
9. Enter **list meas ds1 sum location** to display the bit error count.
10. Repeat Steps 5 through 8 as needed to observe bit error rate characteristics. Also, wait 1 to 10 minutes between Steps 5 through 7. One minute without errors translates to greater than a 1 in 10 to the eighth error rate. Ten minutes without errors translates to greater than a 1-in-10^9 error rate.
11. 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.

12. Terminate the test by entering **`test ds1-loop location end-loopback/span-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 290for 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`**.

13. Restore the **TX LBO** field to the original value recorded in Step 2.
14. Release the DS1 circuit pack using the **`release board location`** command.
15. Leave the loopback jack connected to the DS1 span.

DS1 span field descriptions

Displayed field	Function	Description
Test: cpe-loopback-jack	Pattern 3-in-24	The loopback jack test is active.
Synchronized	Y or N	• If the system displays y, 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 the system displays n, 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

Displayed field	Function	Description
		be intermittent connections or a broken wire in a receive or transmit pair in the CPE wiring.
Bit Error Count	Cumulative count of detected errors	If there are no wiring problems, the counter remains at 0. 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.

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 Configuring DS1 using a Smart Jack on page 290 and Configuring DS1 without a Smart Jack on page 296.

Configuring DS1 using a Smart Jack

About this task

The addition of the loopback jack and the presence of a Smart Jack divides the DS1 span into three separate sections for fault isolation. 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:

Procedure

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 the figure on page 293) 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 tests on page 287. 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.

DS1 span section descriptions

Name	Description
Section 1:	Between the 120A ICSU and the loopback jack
Section 2:	Between the loopback jack and the Smart Jack (network interface point)

Name	Description
Section 3:	From the Smart Jack to the Central Office (CO). It is necessary to contact the DS1 provider to run this test.

Smart Jack Network Interface

When the loopback jack is added to a span that does not contain a Smart Jack, the span is divided into two sections. See the figure on page 297 and the figure on page 298. These sections are described in the table on page 292.

Table 57: 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)

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 the 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.

Network Interface at Smart Jack

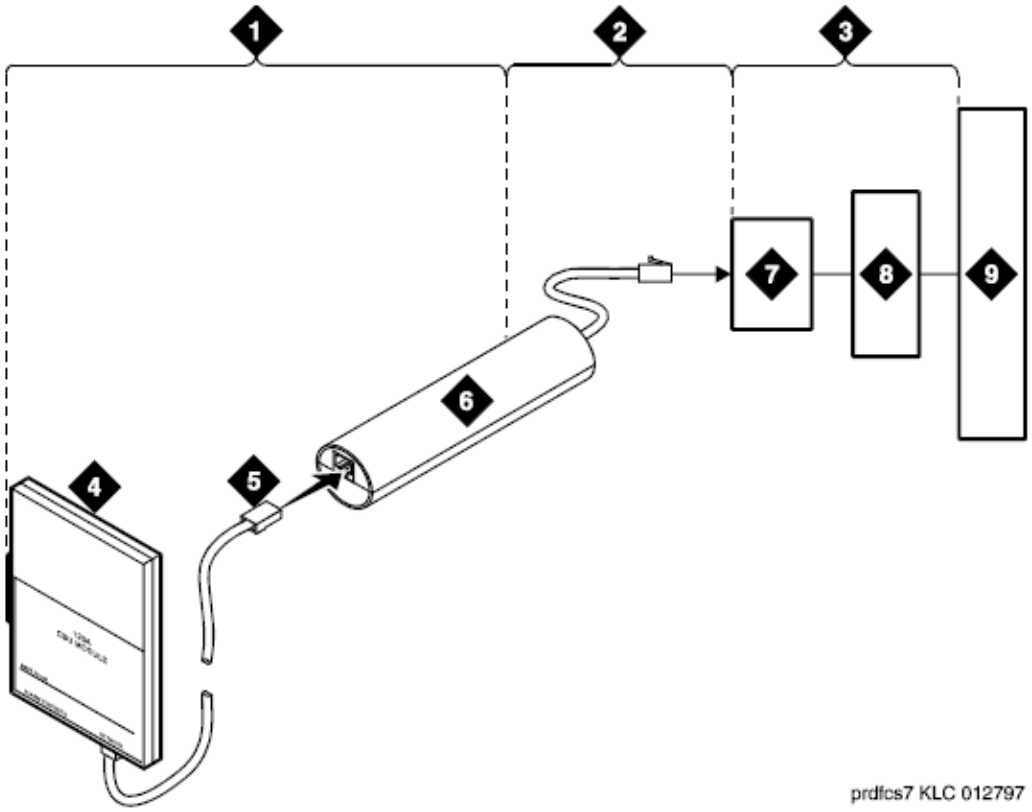


Figure 52: Network Interface at Smart Jack

Number	Description
1	Span Section 1
2	Span Section 2
3	Span Section 3
4	120A Integrated Channel Service Unit (ICSU)
5	RJ-48 to Network Interface (Up to 1000 Feet) (305 m)
6	Loopback Jack
7	Network Interface Smart Jack
8	Interface Termination of Fiber MUX
9	Central Office

Extended Demarcation Point Network Interface (Smart Jack Inaccessible)

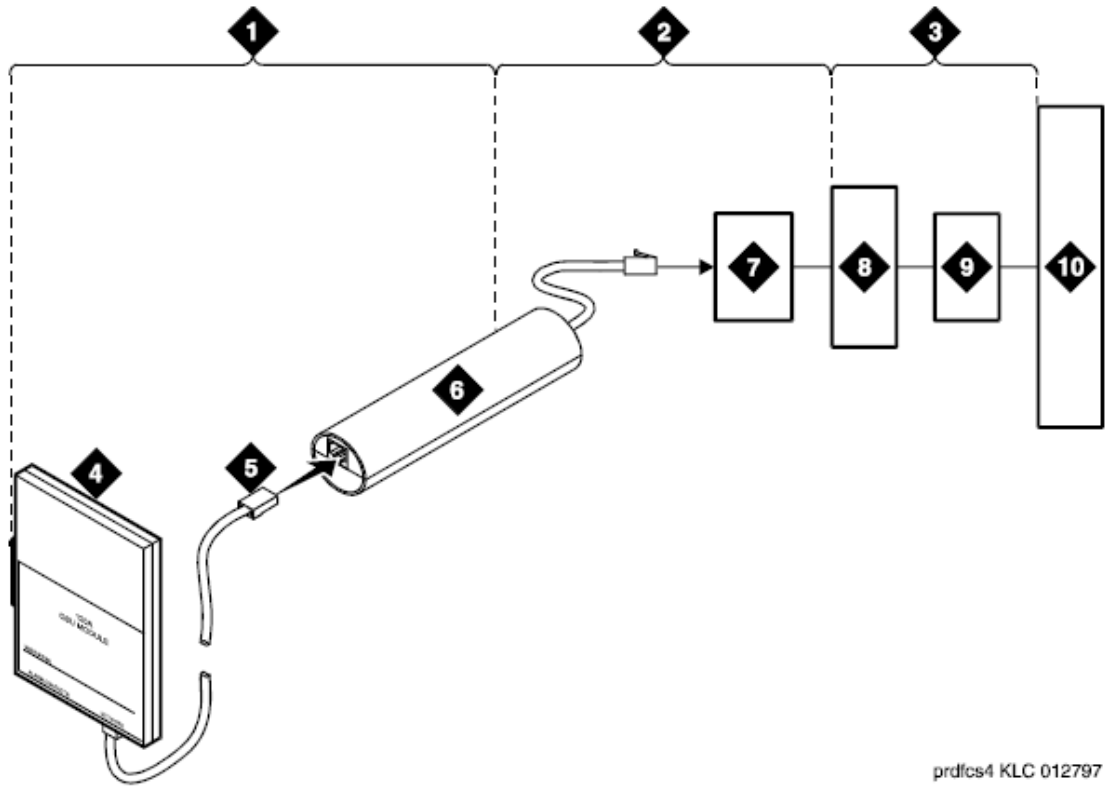


Figure 53: Network Interface at Extended Demarcation Point (Smart Jack inaccessible)

Number	Description
1	Span Section 1
2	Span Section 2
3	Span Section 3
4	120A Integrated Channel Service Unit (ICSU)
5	RJ-48 to Network Interface (up to 1000 Feet) (305 m)
6	Loopback Jack
7	“Dumb” Block (Extended Demarcation)
8	Network Interface Smart Jack
9	Interface Termination or Fiber MUX
10	Central Office

Extended Demarcation Point Network Interface (Smart Jack Accessible)

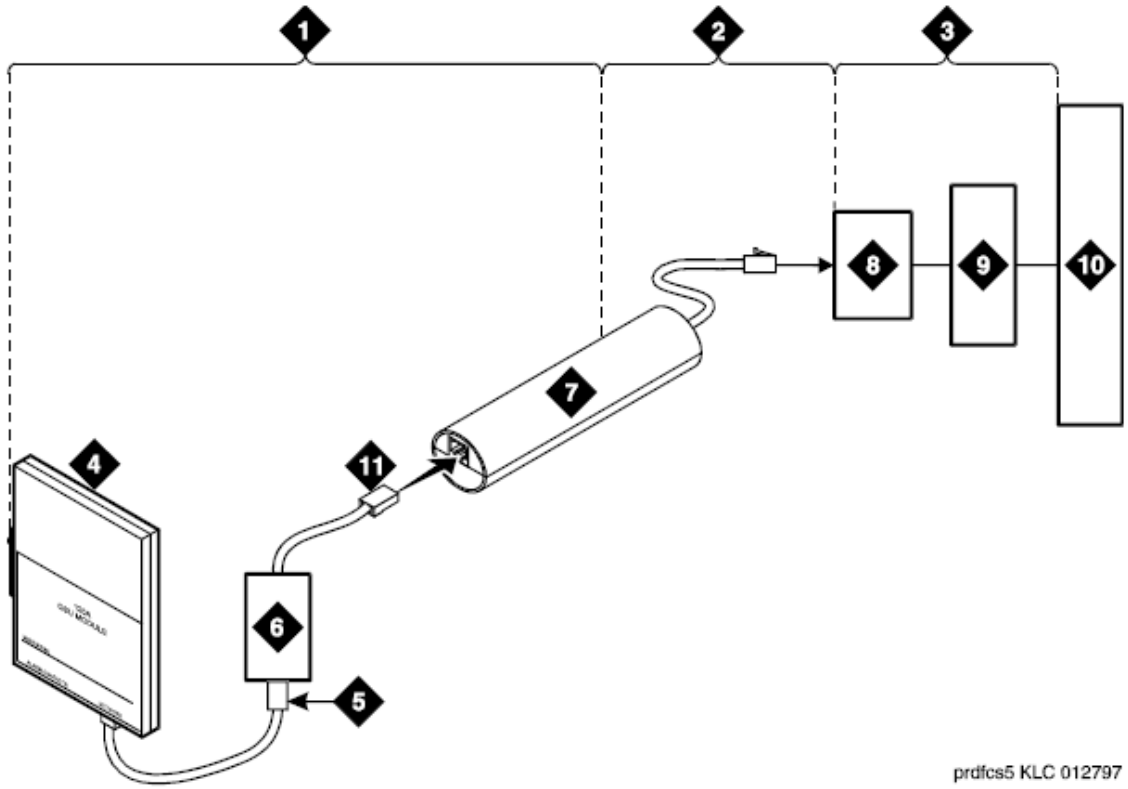


Figure 54: Network Interface at Extended Demarcation Point (Smart Jack accessible)

Number	Description
1	Span Section 1
2	Span Section 2
3	Span Section 3
4	120A Integrated Channel Service Unit (ICSU)
5	RJ-48 to Network Interface (up to 1000 Feet) (305 m)
6	Dumb Block (Extended Demarcation)
7	Loopback Jack
8	Network Interface Smart Jack
9	Interface Termination or Fiber MUX

Number	Description
10	Central Office
11	Dumb Block to Smart Jack RJ-48

Configuring DS1 without a Smart Jack

About this task

Testing is divided into two steps:

Procedure

1. Test customer premises wiring (section 1 in the figure on page 297) from the ICSU to the loopback jack as described in DS1 span tests on page 287.
2. Test the loopback jack-to-dumb block and dumb block-to-CO wiring (Span Section 2 in the figure on page 297). 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.

Dumb Block Network Interface

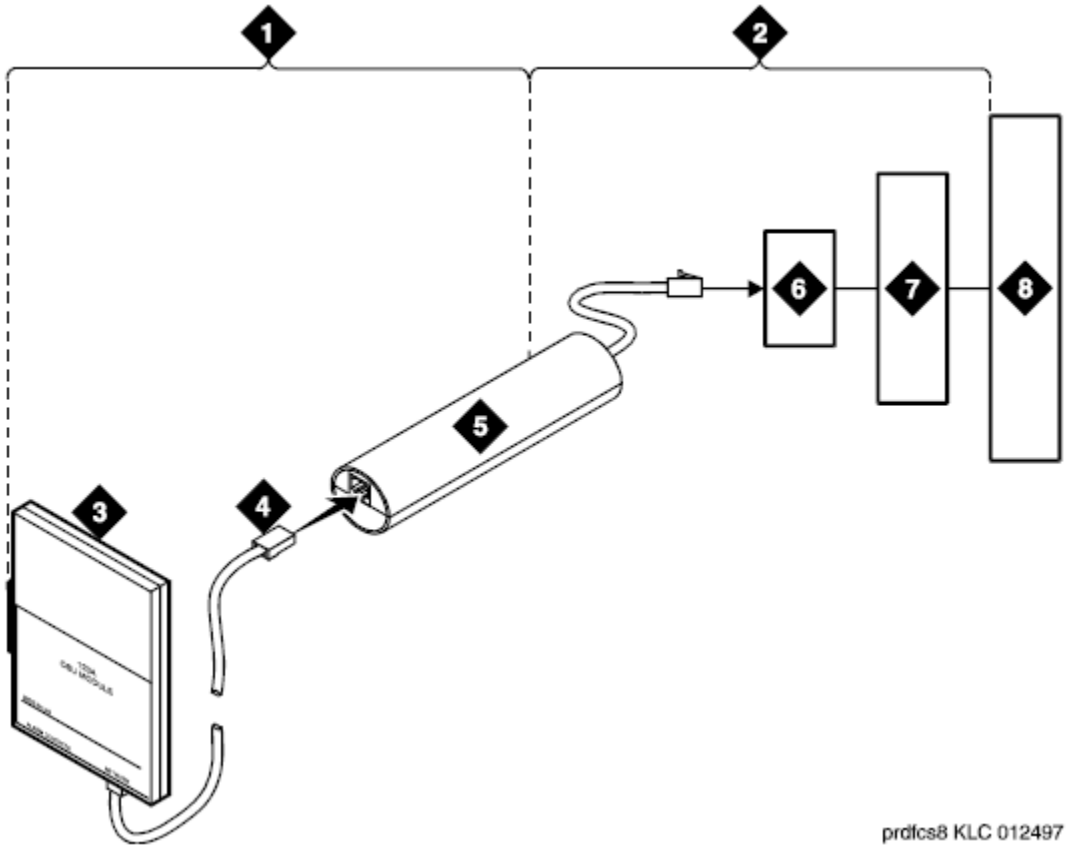


Figure 55: Network Interface at Dumb Block

Number	Description
1	Span Section 1
2	Span Section 2
3	120A Integrated Channel Service Unit (ICSU)
4	RJ-48 to Network Interface (up to 1000 Feet) (305 m)
5	Loopback Jack

6	“Dumb” Block (Demarcation Point)
7	Interface Termination or Fiber MUX
8	Central Office

Dumb Block with repeater line to Fiber MUX Network Interface

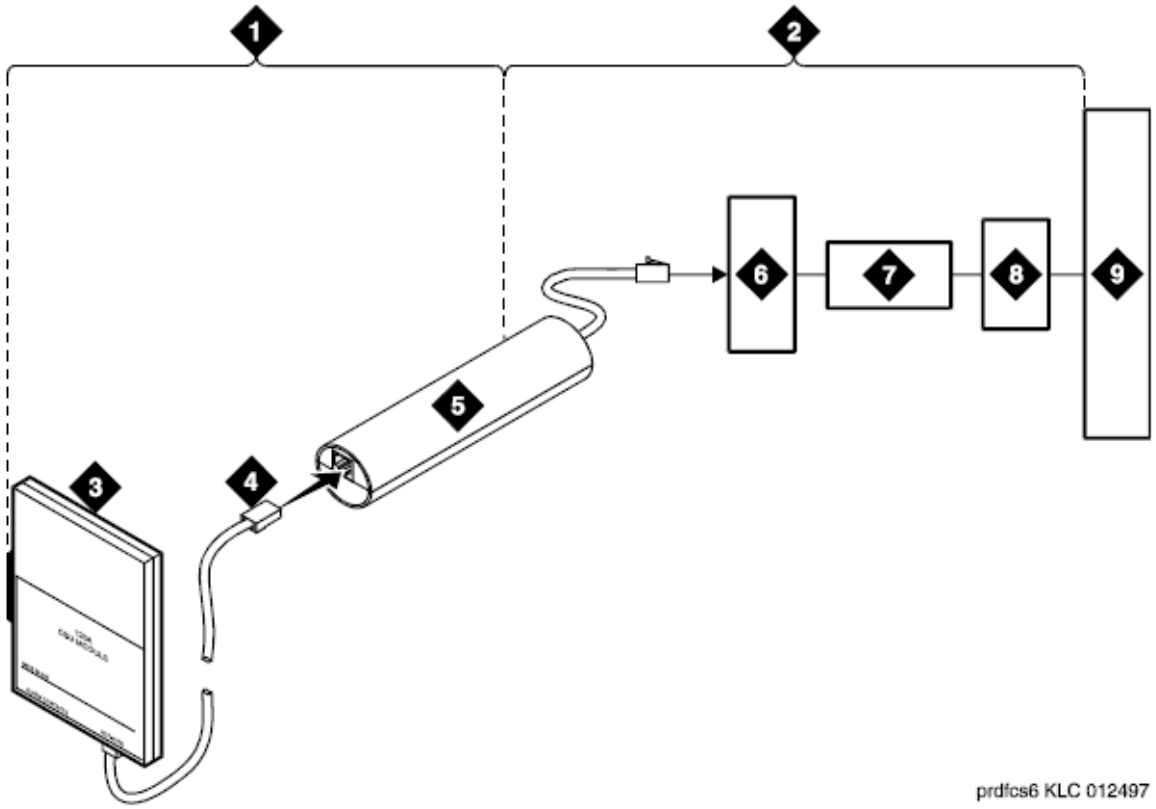


Figure 56: Network Interface at Dumb Block with repeater line to Fiber MUX

Number	Description
1	Span Section 1
2	Span Section 2
3	120A Integrated Channel Service Unit (ICSU)
4	RJ-48 to Network Interface (up to 1000 Feet) (305 m)
5	Loopback Jack
6	“Dumb” Block (Demarcation Point)

7	Repeater
8	Fiber MUX
9	Central Office

Fiber multiplexers testing configurations

You can use the loopback jack when customer premises DS1 wiring connects to an onsite 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. These spans must be tested by using the same procedures as metallic spans.

Note:

Fiber MUXs might have loopback capabilities that can be activated by the service provider from the CO end. These might 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 might be activated following a successful loopback jack test and used to isolate problems to the wiring between the loopback jack and the MUX.

Voltage:

Installations that use repeated metallic lines between the MUX and the “dumb” block require DC power for the repeaters. 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.

You can make the following four measurements at the network interface jack, to check for the presence of DC:

- From Transmit Tip (T, Pin 5) to Receive Tip (T1, Pin 2)
- From Transmit Ring (R, Pin 4) to Receive Ring (R1, Pin 4)
- From Transmit Tip (T, Pin 5) to Transmit Ring (R, Pin 4)
- From Receive Tip (T1, Pin 2) to Receive Ring (R1, Pin 4)

Every measurement should read 0 (zero) volts DC. For more information, see *Avaya Aura*® *Communication Manager Overview and Specification*.

Facility test calls

Using the facility test calls feature, you can 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**. The system displays the code on page 1 of the screen output.

Note:

For the ISDN-PRI test call feature see ISDN-PRI test calls troubleshooting on page 165.

The test call descriptions mentioned below are for voice terminal users.

Trunk test call

Using the facility test call feature, you can 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**. The system displays the code on page 1 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.

Placing a test call

Procedure

1. Dial the Feature Access Code (FAC) described above and listen for dial tone.
2. Duplicated servers: If the trunk is on a Duplicated Server 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. S8300D/G450 and G430: If the trunk is on a G450 and G430 MM710 Media Module, dial the 7-digit port location MMMVXyy, where:

   - MMM = 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 S8300D 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/MM714/MM716), 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 *Avaya Aura® Communication Manager Overview*.

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. Using this DS0 loop around, a network service provider can 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:

- You can set the communications type to data when the incoming trunk group is used only for data calls (SDS).
- You can 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).
- You can 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.

Placing a tone receiver test call

Procedure

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:
   - Confirmation tone: The DTMR is connected. Go to the next step.
   - Intercept tone: The port entered is not a TTR or the board is not inserted (if a trunk, see above).
   - Reorder tone: The DTMR is in use (call processing), the board is busied out, or inter-PN resources are unavailable for the call.
   - Dial tone: The port is a trunk. See the preceding section.

   Note:

   For a definition of call progress tones, refer to *Avaya Aura® Communication Manager Overview*.
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 1 through 3.
6. To terminate the test call, disconnect 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 305.

Testing a specific time slot on the TDM bus

About this task

Use this procedure to test a specific time slot on the TDM bus of a specific port network.

Procedure

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 58: TDM Bus time slot numbers on page 305.
3. Listen for one of the following call progress tones:
   - 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 58: TDM Bus time slot numbers on page 305.

Note:

For a definition of call progress tones, refer to *Avaya Aura® Communication Manager Overview*.

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 buses (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 buses is busy.

Table 58: TDM Bus time slot numbers

TDM Bus A time slot	TDM Bus B time slot	Tone heard
000	256	Reorder
001	257	Reorder
002	258	Reorder
003	259	Reorder
004	260	Reorder
005	261	Touch Tone 1 — 697 Hz
006	262	Touch Tone 2 — 770 Hz
007	263	Touch Tone 3 — 852 Hz
008	264	Touch Tone 4 — 941 Hz
009	265	Touch Tone 5 — 1209 Hz
010	266	Touch Tone 6 — 1336 Hz
011	267	Touch Tone 7 — 1447 Hz
012	268	Touch Tone 8 — 1633 Hz
013	269	Dial Tone
014	270	Reorder Tone
015	271	Alert Tone
016	272	Busy Tone
017	273	Ringback Tone
018	274	Special Ringback Tone
019	275	2225-Hz Tone
020	276	Music
021	277	Tone on Hold
022–253	278–509	Confirmation (used for calls)
254	510	Reorder
255	511	Confirmation

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.

Placing a call to test out-of-service time slot

Procedure

1. Dial the FAC described above and listen for dial tone.
2. Dial the port network number followed by ****.

   If you can hear a reorder tone, there are no out-of-service time slots on the specified port network.

   If you hear a confirmation tone, connection is made to an out-of-service time slot.
3. Repeated test calls will alternate between out-of-service time slots on TDM bus A and TDM bus B.

Placing a call to test the system tone

About this task

Use this procedure for placing a call to connect the voice terminal to a specific system tone.

Procedure

1. Dial the FAC described above.
2. Dial the port network number followed by * and the two-digit tone identification number from the table on page 307.

   If you hear an intercept tone, the number entered is not a valid tone number. If you hear a reorder tone, inter-PN resources are not available. If you hear a system tone, the specified tone will be heard if it is functioning.

   Note:

   For a definition of call progress tones, refer to *Avaya Aura® Communication Manager Overview*.

List of system tone identification numbers

Number	Description
00	Null tone
01	Dial tone
02	Reorder tone
03	Alert tone
04	Busy tone
05	Recall dial tone
06	Confirmation tone
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

Number	Description
28	External call waiting
29	Priority call waiting
30	Busy verification
31	Executive override/intrusion tone
32	Incoming call identification
33	Dial zero
34	Attendant transfer
35	Test calls
36	Recall on don’t answer
37	Audible ring
38	Camp-on recall
39	Camp-on confirmation
40	Hold recall
41	Hold confirmation
42	Zip tone
43	2804 Hz
44	1004 Hz (-16db)
45	1004 Hz (0 db)
46	404 Hz
47	Transmission test sequence 105
48	Redirect tone
49	Voice signaling tone
50	Digital milliwatt
51	440 Hz + 480 Hz
52	Music
53	Transmission test sequence 100
54	Transmission test sequence 102
55	Laboratory test tone 1
56	Laboratory test tone 2
57	Disable echo supervision dial tone
58	7 seconds of answer tone

Number	Description
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

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.

Server UPS batteries

For information about maintaining the batteries that support the Duplicated Servers, refer to the User's Guide or other product documentation that ships with the UPS. You can use the following table to enter the data.

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.						

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. Using this testing configuration, you can connect tie trunks back-to-back in the same switch to verify the operation of tie trunk ports. The tests can be performed using one of the following procedures:

- Testing E&M mode
- Testing Simplex mode

Testing using the E&M mode

Procedure

1. At the administration terminal, enter `list configuration trunks` to determine which ports are assigned on the Tie Trunk circuit pack.
2. Enter `display dialplan` to determine the Trunk Access Code (TAC) format.
3. Enter `display port xxx` for every port defined in Step 1.

This lists the trunk groups of which the ports are members. For details about removing and replacing port circuit packs, see Server circuit packs reseat and replacement on page 232.

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.
10. In the Group Type field, enter `tie`.
11. In the TAC field, enter the trunk access code obtained from dial plan.
12. In the Trunk Type (in/out) field, enter `wink/wink`.
13. In the Port field, assign two of the ports from the tie trunk.
14. In the Mode field, enter E&M for both ports.
15. In the Type field, enter `t1-stan and t1-comp` (t1 standard and t1 compatible).
16. 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.
17. 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.
18. 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 on page 311 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 in the *Ports Wiring* table.
19. Check all wirings to verify good connections between the two test ports.
20. 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.

21. 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.
22. Disconnect the jumpers between two ports. Then use administration terminal and trunk printouts to restore every trunk-group change to normal values.

Ports wiring E&M mode

Table 59: Ports wiring

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

Carrier lead appearances MDF

110 connecting block terminals	CO Trunk TN747	Tie Trunk TN760
1	T1	T1
2	R1	R1
3		T11
4		R11
5		E1
6		M1
7	T2	T2
8	R2	R2
9		T12
10		R12
11		E2
12		M2

110 connecting block terminals	CO Trunk TN747	Tie Trunk TN760
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		
30		
31	T6	
32	R6	
33		
34		
35		
36		
37	T7	
38	R7	
39		
40		
41		
42		
43	T8	

110 connecting block terminals	CO Trunk TN747	Tie Trunk TN760
44	R8	
45		
46		
47		
48		
49		
50		

Testing using the Simplex mode

Procedure

1. Repeat steps 1 through 7 of the Testing using the E&M mode procedure.
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.
4. In the Group Type field, enter `tie`.
5. In the TAC field, enter the trunk access code obtained from dial plan.
6. In the Trunk Type (in/out) field, enter `wink/wink`.
7. In the Port field, assign two of the ports from the tie trunk.
8. In the Mode field, enter simplex for both ports.
9. In the Type field, enter type-5 (5 compatible).
10. 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.
11. 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.
12. Use jumper wires (DT 24M-Y/BL/R/G) and the D impact tool to connect wiring between the two ports assigned in Step 10 on page 314 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 in the *Ports wiring simplex mode* table.

13. Repeat Steps 13 through 16 of the Testing using the E&M mode on page 310.

Ports wiring simplex mode

Table 60: Ports wiring

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

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 (the table on page 315 and the table on page 316), set the switches on the TN760E and administer the port using the figure on page 316 and the table on page 317.

Signaling formats for TN760E

Table 61: 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

Signaling type summary

Table 62: 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.				

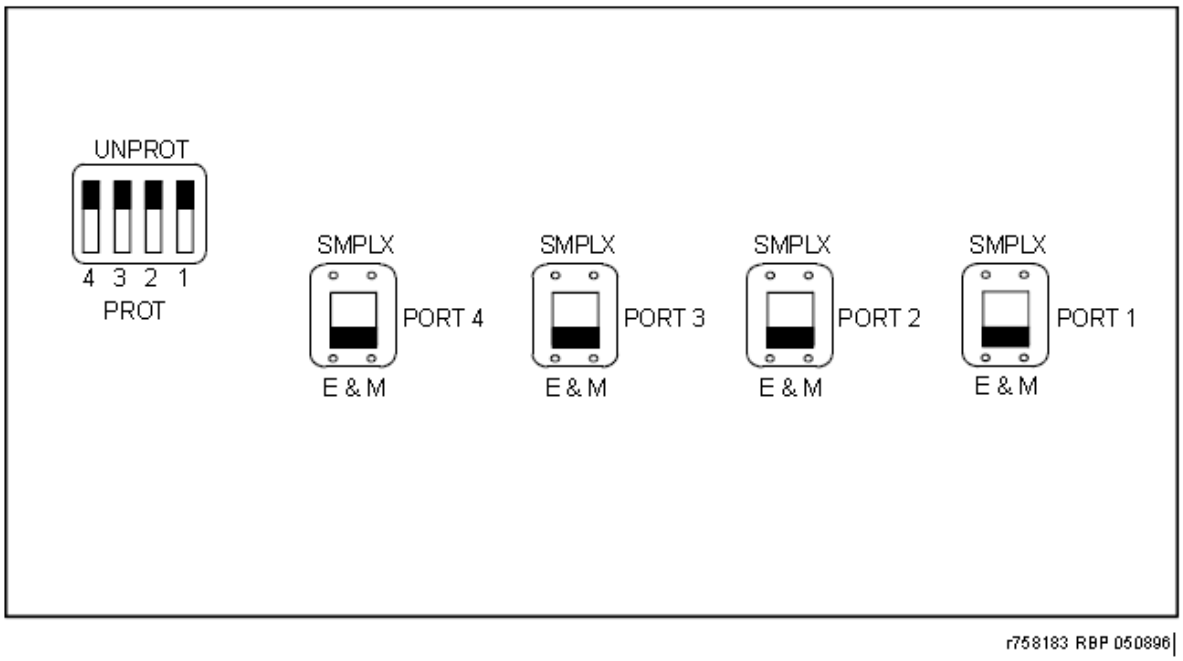


Figure 57: TN760E tie trunk circuit pack (component side) (R758183)

Table 63: TN760E option switch settings and administration

Installation situation		Preferred signaling format		E&M/ SMPLXswitch	Prot/ Unprotswitch	Administered port
Circumstance	To	System	Far-End			
Co-Located	Avaya PBX	E&M Type 1	E&M Type 1	E&M	Unprotected	Type 1
		Compatible	Standard			Compatible
Inter-Building	Avaya PBX	Protected Type 1	Protected Type 1	E&M	Protected	Type 1
		Compatible	Standard Plus			Compatible
			Protection			
			Unit			
Co-Located	Net Integrated	E&M Type 1	Any PBX	E&M	Unprotected	Type 1
		Standard				

TN464E/F option settings

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 the table on page 317 and the figure on page 318.

Table 64: 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

TN464E/F option

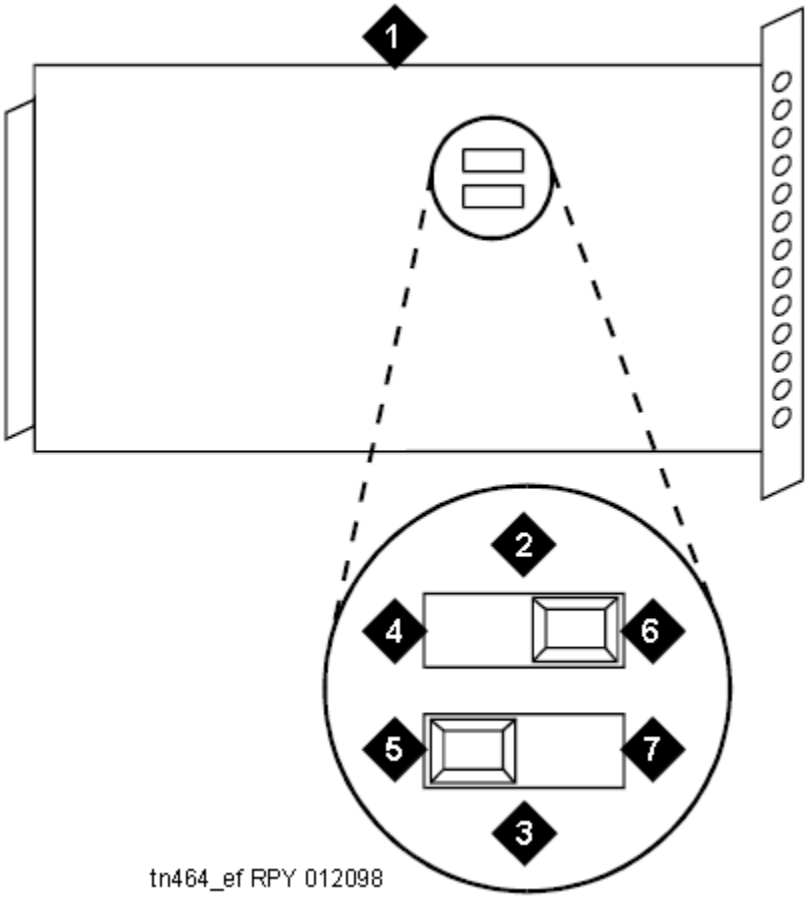


Figure 58: TN464E/F option settings

Number	Description
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 S8300D 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 as per the administered time interval.

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

Power removal and restoration

Caution:

Before turning off a cabinet or carrier with the Communication Manager Messaging application enabled (S8300D), first stop the Communication Manager Messaging application to avoid corruption of the application's LDAP database. For instructions on stopping the application, see the Communication Manager Messaging documentation, and in Hot swapping media modules on page 47.

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 multicarrier cabinets

Procedure

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-POR (ASAI ISDN-BRI Port) in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 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 and restoring power to Gateways

Procedure

1. Turn off S8300D Server, if installed.To shut down S8300D Server, you must press the shutdown button and wait for 2–3 minutes until the OK-to-remove LED turn on.
2. Disconnect the power supplies from the mains power source:
   a. Disconnect the AC power cables to the inlet receptacle on the rear of the chassis.
   b. Disconnect the other end of the power cables into a mains socket.

Removing and restoring power to the mains power source

About this task

Use this procedure to restore power, reconnect the power supplies to the mains power source.

Procedure

1. Connect the AC power cables to the inlet receptacles on the rear of the chassis.
2. Connect the other end of the power cables into a mains socket.

Duplicated Series Server power removal and restoration

Always shut down the Avaya Duplicated Series servers from the System Management Interface (SMI) 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 Duplicated Servers

Shutting down the Off Line (standby) server

About this task

Use this procedure to shut down a Duplicated Off Line (standby) server for maintenance.

Procedure

1. Log in to the System Management Interface (SMI) for the Off Line (standby) server.
2. Select **Data Backup/Restore** > **Backup Now** and backup the data.
3. Select **Server** > **Busy-Out/Release Server** from the main menu.
   The Busy-Out/Release Server page displays.
4. 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.
5. Select **Server** > **Shutdown Server** from the main menu.
   The Shutdown Server page displays.
6. Select **Immediate Shutdown** and clear **Restart server after shutdown**.
7. Click the **Shutdown** button and wait until the server powers down.
8. When both of the servers are powered down, remove the power.

Result

To restore power, see Restoring power to the Duplicated Servers on page 323.

Shutting down the server pair

About this task

Use this procedure to shut down both the On Line (active) and Off Line (standby) servers.

Procedure

1. Log in to the System Management Interface (SMI) for the Off Line (standby) server.
2. Select **Data Backup/Restore** > **Backup Now** and backup the data.

Note:

This procedure shuts down both servers and terminates Communication Manager, meaning that the entire telephone system is inoperable including Emergency Transfer. Users cannot make any telephone calls.

3. Select **Shutdown Server** from the main menu.
   The Shutdown This Server page displays.
4. Select **Immediate Shutdown** and clear **Restart server after shutdown**.
5. Press the **Shutdown** button and wait until the server has powered down.
6. On the System Management Interface (SMI) for the On Line (main) server select **Data Backup/Restore** > **Backup Now** and backup the data.
7. Select **Server** > **Shutdown Server** with these options:
   - Select the Immediate Shutdown option.
   - Select **Shutdown even if this is active server (or Shutdown even if this is the standby server and it is not busied out)**.
   - Do not select **Restart server after shutdown**.
8. Click **Shutdown** and wait until the server powers down.
9. When both of the servers are powered down, remove power from the servers.

Result

To restore power, see Restoring power to the Duplicated Servers on page 323.

Restoring power to the Duplicated Servers

About this task

Use this procedure to restore power to the Duplicated server.

Procedure

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.

Neon voltage (ring ping)

Setting the neon voltage 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.

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.

Adjusting the neon voltage

About this task

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 this procedure to adjust the neon voltage.

Procedure

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 the figure on page 325. 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.

Setting the neon voltage

About this task

Use the knob as shown in the figure to adjust the neon voltage.

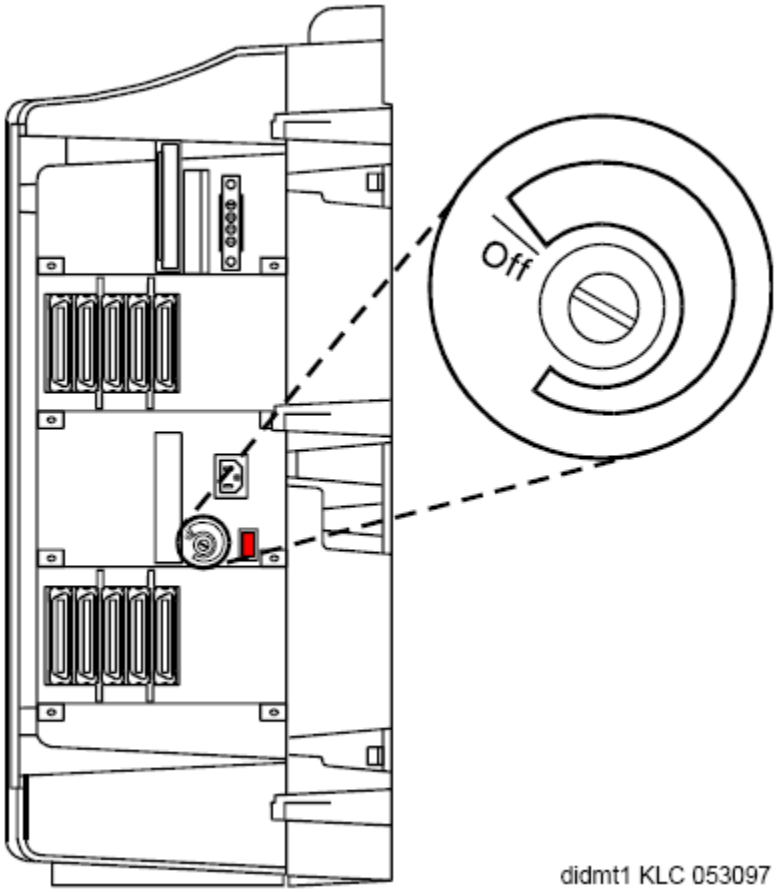


Figure 59: Setting the neon voltage

Removing power on the G450 and G430 gateways

About this task

The G450 and G430 gateways contain a detachable power cord. Use this procedure to remove power on the G450 and G430 gateways.

Procedure

1. Add power by plugging the power cord into the G450 and G430 receptacle.
2. Plug the cord into the wall outlet.

Restoring power on the G450 and G430 gateways

About this task

Use this procedure to restore power on the G450 and G430 gateways.

Procedure

1. Remove power by properly powering down the S8300D (if the G450 and G430 is equipped with an S8300D).
2. Unplug the power cord from the wall outlet and from the G450 and G430 receptacle.

Note:

The power supply in the G450 and G430 gateways is not replaceable.

Note:

Auxiliary power is currently unavailable on the G450 and G430 gateways.

Shutting down an active or a functional but inactive Survivable Remote Server

About this task

Use this procedure to shut down an active or a functional but inactive Survivable Remote Server.

Procedure

1. Under Server, click **Shutdown This Server**.
2. On the Shutdown This Server screen, system restart check boxes 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

3. Accept the default option.
4. Leave the check box **After Shutdown, Restart System** cleared.
5. Click **Shutdown**.

Note:

If the normal shutdown procedure does not succeed, when pressed, the shutdown button programs the S8300D 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 S8300D for later analysis.

Shutting down an active or a functional but inactive Survivable Remote Server manually

About this task

Use this procedure to shut down an active or a functional but inactive Survivable Remote Server.

Procedure

Keep the button located next to the fourth GREEN Ok-to-Remove LED (specific to the S8300D), pressed for two seconds.

- For Communication Manager versions 1.2 and earlier, the fourth GREEN Ok-to-Remove LED flashes at a constant rate until it finally glows steadily.
- For Communication Manager version 1.3 and later, the fourth GREEN “Ok-to-Remove” LED flashes at a constant rate, and the TST LED flashes slowly at first. As computer processes exit, the TST LED flashes faster. When the shutdown has completed, the TST LED goes out, and the “OK to Remove” LED then glows steadily.

Once steady, this GREEN “Ok-to-Remove” LED indicates that the disk drive has been parked properly and the S8300D is ready to be removed.

Note:

The two processes described below apply to Communication Manager version 1.3 and later.

LED sequence for shutdown failure with successful recovery

If a high priority process has seized control of the S8300D processor, the shutdown signal might be held up indefinitely. After 80 seconds, the system runs a recovery function within the

S8300D operating system that equalizes process priorities, and allows the shutdown sequence to proceed. The LED sequence is:

- After the shutdown button is pressed and held for at least two seconds, the **OK to Remove** LED light flashes constantly. The TST LED flashes slowly at first.
- 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.
- As processes exit, the TST LED flashes faster, and the YELLOW ACT LED remains illuminated.
- As shutdown completes, the TST LED goes out, and the **OK to Remove** LED comes on steady. At this point, it is safe to remove the S8300D module from the G450 and G430.

LED sequence for complete shutdown failure

If an operating system level failure has occurred, it is possible that the processor will never allow the shutdown to begin, even after process priorities are equalized by the recovery function at the 80 second interval. After two minutes, the hardware watchdog resets the S8300D. The LED sequence is as:

- 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.
- 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.
- 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 S8300D. At this point, the RED ALM LED is illuminated and all others go out. Although this begins restarting the S8300D, it will be safe to remove the S8300D module from the G450 and G430 gateways 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 335 or ATMS detail report on page 337.

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 test

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. The table on page 330 shows which tests are run for each type of TTL.

ATMS tests use 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)

Enabling ATMS tests

About this task

Use this procedure to set the administrative prerequisites to enable testing.

Procedure

Use the ATMS administration table to set the fields for enabling testing.

Table 65: ATMS administration

Screen	Field	Value
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
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

Input parameters analog test call

Table 66: Input parameters (analog test call)

Input	Description
trunk addresses	Specify a single trunk or several trunks by using trunk, port, or board addresses. If you enter a trunk-group number without a member number, every member of the group is tested.

Input	Description
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 1 on page 0 .

Different TTLs have different measurement capabilities, and you will need the information about specific TTL types in the table on page 331, which does not include the self-test nor does it distinguish between measurements for different test tone levels.

Table 67: Measurement capability by TTL type

	Terminating Test Line Type				
Test	**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			

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
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-POR (ASAI ISDN-BRI Port) in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 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 test calls can be retrieved with the **`list testcalls`** command as described in ATMS reports on page 334. The measurements that are made and recorded depend on the type of test that is specified and the capabilities of the far-end TTL.

The figure on page 333 shows a typical result 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
```

Figure 60: Test results for test analog-testcall trunk 60

Test result field descriptions

Name	Description
Port	The physical location of the port supporting the trunk being tested.
Maintenance Name	The name of the maintenance object tested, TIE-TRK or CO-TRK.
Alt. Name	The trunk-group number and member number of the trunk being tested.
Test Number	ATMS tests are numbered 844 through 848.
Result	• If the test call successfully completes, and if every trunk tests within administered thresholds for marginal and unacceptable performance, then a PASS result is returned. • 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-POR (ASAI ISDN-BRI Port) in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

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 332 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

Name	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.

Name	Description
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. The figure on page 336 shows a typical summary report.

```
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
```

Figure 61: ATMS Summary Report screen

Output field and descriptions

Name	Description
Trk Grp Num	Results for each trunk group are listed by trunk-group number. Only outgoing or 2-way analog trunks are listed.
Num Of Trks	The number of members in the trunk group.
Last Test Date	The date of the oldest measurement in the trunk group.
Last Test Time	The time of the oldest measurement in the trunk group.
Trunks Passed Transm Test	The number of trunks that have passed the trunk transmission tests.
Trunks Failed Marginal Threshld	The number of trunks that performed outside the marginal threshold, but not the unacceptable threshold, as defined on the Trunk Group screen.
Trunks Failed Unaccept Threshld	The number of trunks that performed outside the unacceptable threshold, as defined on the Trunk Group screen.
Trks In-Use	The number of trunks that were in use at the time of testing. Abort codes for trunk-in-use are 1000 and 1004.
Trks Not Test	The number of trunks that were not tested due to error conditions other than trunk-in-

Name	Description
	use. Abort codes are given in the detailed report.
Busied Out Trunks	The number of trunks that were busied out in response to test failures. These may be caused by hardware problems, incorrect threshold values, and so on.

ATMS detail report

This report is divided into two sections. The upper section lists the trunk group, trunk type, trunk vendor, TTL type, and the user-defined threshold values administered on page 4 of the Trunk Group screen (the figure on page 337). 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.

```
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
```

Figure 62: ATMS detail report

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.

Name	Description
Group	The trunk-group number selected

Name	Description
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-POR (ASAI ISDN-BRI Port) in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430. • blank: indicates that no measurements have been made on this trunk since the database was last initialized.
1004Hz-lossMin	Far-to-near and near-to-far measurements of 1004-Hz loss from low-level tone.
1004Hz-loss Max	Far-to-near and near-to-far measurements of 1004-Hz loss at 0 dBm.
Loss dev at 404Hz	These low-frequency transmission tests measure maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements.

Name	Description
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.

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.

IP telephones troubleshooting

Note:

Refer to these documents for troubleshooting details and error codes, as well as the telephone administration information:

- *4606 IP Telephone User's Guide*
- *4624 IP Telephone User's Guide*
- *4612 IP Telephone User's Guide*
- *Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.2 for 9608, 9611G, 9621G,and 9641G IP Deskphones, 16-603504*
- *Avaya one-X® Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones, 16-603596*
- *Avaya one-X® Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide Release 6.2, 16-601944*

The Avaya 4600-Series IP Telephones are relatively trouble-free. The following troubleshooting sections provide 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:

Tip:

Telephone does not activate after connecting it the first time

Telephone does not activate after a power interruption

After you unplug or power down the telephone server problems or other power interruption may be caused.

Activating telephone after power interruption

Procedure

Allow a few minutes for re-initialization.

Characters do not appear on the display screen

The characters may not be appearing your screen because of the power source interruption.

Displaying characters on the screen

Procedure

1. Check the power source to be sure your telephone is receiving power.
2. Check all lines into the telephone to be sure it is properly connected.
3. Keeping the telephone idle, press and hold the **Trnsfr** button; the line/feature indicators should light and the display should show all shaded blocks.
4. Release the **Trnsfr** button to end the test.
5. If the above suggested solutions do not resolve the problem, reset or power cycle the telephone.

Display shows an error/informational message

Most messages involve server/telephone interaction. If you cannot resolve the problem based on the message received, contact your Telephone System Administrator for resolution.

Unable to get the dial tone

The dial tone of the telephone may have been stopped because of the causes listed below:

- Headset and line cord are not connected securely
- Telephone is not powered
- Telephone is not communicating with the switch

Activating the telephone

Procedure

1. Make sure both the handset and line cords into the telephone are securely connected.

   Note that there may be a slight operational delay if you unplug and reconnect the telephone.
2. If you have a 4612 or 4624 IP Telephone, check to be sure the telephone is powered (press `Menu`, then `Exit`); if the system does not display anything on the display, check your power source.
3. If you have a 4612 or 4624 IP Telephone, check to be sure your telephone is communicating with the switch; press `Menu`, then any of the softkey features (for example, Timer). If the selected feature activates, the switch/IP telephone connection is working.
4. Reset or power cycle the telephone.
5. See your Telephone System Administrator if the above steps do not produce the required result.
6. Check the status of the VoIP board.

Echo, noise or static is heard while using a headset

You might be hearing an echo, noise, or static while using the headset because of the causes listed below:

- Headset connection is not secure
- Headsets, base unit, or adapter are not approved

Improving clarity of sound while using a headset

Procedure

1. Check the headset connection.
2. If the connection is secure, verify that you are using an approved headset, base unit or adapter, as described in the list of approved Avaya Communication compatible Headsets.

Telephone does not ring

The telephone may not be ringing because of the causes listed below:

- Telephone is set to Ringer Off
- Ringer volume is low

Activating the telephone ring

Procedure

1. If you have a 4612 or 4624 IP Telephone, use the Menu to access the RngOf (Ringer Off) feature; if the system displays a carat (downward triangle) above that feature, your telephone is set to not ring. To correct, press the softkey below RngOf; when the carat does not display, your ringer is active.
2. 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.
3. Set your ringer volume to a higher level using the Up/Down Volume keys.
4. From another telephone, place a call to your extension to test the above suggested solutions.

Speakerphone does not operate

Activating speaker phone

Procedure

Ask your System Administrator if your speakerphone has been disabled.

A feature does not work as indicated in the User Guide

A feature may not be working on your telephone because your telephone is specifically programmed for certain features only.

Activating any feature

Procedure

1. Verify the procedure and retry.

For certain features, you must lift the handset first or place the telephone off-hook.

2. See your Telephone System Administrator if the above action does not produce the required result; your telephone system may have been specially programmed for certain features applicable only to your installation.

Resetting an IP Telephone

About this task

Reset your IP Telephone when other troubleshooting suggestions do not correct the problem. This basic reset procedure should resolve most problems.

Use this procedure to reset your telephone.

Procedure

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 the table on page 344:

   Table 68: Resetting the IP Telephone

If you want to	Then
Reset the telephone without resetting any assigned values	Press * (asterisk). A confirmation tone sounds and the display prompts `Restart phone? * = no # = yes`.
Reset the telephone and any previously assigned (programmed) values (Use this option only if your telephone 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 telephone or `*` to terminate the restart and restore the telephone to its previous state.

Note:

Any reset/restart of your telephone 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

About this task

Power cycle with the approval of your System Administrator only when a reset does not resolve the problem. Use the power cycle only if the basic or programmed reset procedure cannot be performed or does not correct the problem.

Procedure

1. Unplug the telephone and plug it back in.

   The telephone connection re-establishes.

2. If power-cycling does not correct the problem, perform a more severe power cycle routine by unplugging both the telephone and the Ethernet cables.

   Note:

   This type of power cycle involves reprogramming certain values so it should only be performed by your System Administrator.

9608, 9611G, 9621G, and 9641G SIP Deskphones related documents

- For information on troubleshooting Error Conditions and Installation Error and Status Messages, see *Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.2 for 9608, 9611G, 9621G,and 9641G IP Deskphones, 16-603504*.
- *Avaya one-X® Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones, 16-603596*
- *Avaya one-X® Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide Release 6.2, 16-601944*
- For information on software and hardware specifications, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207

Index

Numerics

120A ICSU 291
3-in-24 pattern 288
802.1p QoS and IP DiffServ 151
  verify consistent usage 151
9608, 9611G, 9621G, and 9641G 345
  related documents 345

A

ACA, see Automatic Circuit Assurance 155
accessing 185
  system logs 185
ACLs 147
activating 342, 343
  IP telephone 342
  speaker phone 343
  telephone ring 343
activating a feature 343
add new schedule 223
  field descriptions 223
adding or changing 222
  scheduled backup 222
adjusting 324, 325
  neon voltage 324, 325
administering 182, 287
  loopback jack 287
  syslog server 182
administering logging levels 183
  Communication Manager 183
Administrable IPSI Socket Sanity Timeout 100
alarm 26
  alarm reporting 26
Alarm 25
  alarm reporting 25
alarm logs 21
alarms 14, 21, 24
  classifications 24
  logs 21
  maintenance objects (MOs) 24
  notification 14
    ASA 14
American National Standards Institute, see ANSI 39
analog 34, 40
  carrier signal 34
  modem transmission 34
  port, insertion loss 40
Analog Media Module 49
analog test call 330
  input parameters 330
analog tie trunk testing 310
  E&M mode 310
analog trunk/telephone port board Media Module 47
analog-to- 34, 39, 40, 42
  analog 39, 40, 42
    frequency response 39
    intermodulation distortion 40
    peak noise level 42
    quantization distortion loss 40
  digital 34, 39, 40, 42
    coder/decoder 34
    frequency response 39
    intermodulation distortion 40
    peak noise level 42
    quantization distortion loss 40
analyzing 142, 255
  MedPro ping termination 142
  packet bus problem 255
ANSI 39
ARB (Arbiter) Linux process 61
ASAI 164
  troubleshooting 164
ASG 189
  log entries 189
Asynchronous Data Unit (ADU) 34
  proprietary signal 34
ATMS 328, 339
  measurement analysis 339
ATMS detail report 337
  output field descriptions 337
ATMS report 334
  input parameters 334
ATMS summary report 335, 336
  example 335
  output field descriptions 336
ATMS test calls 329
  test schedule command 329
ATMS tests 329
  enabling 329
Audio Connection Type field 132
audio quality problems 148
Auto Fallback to Primary 73
Automatic Circuit Assurance (ACA) 155

automatic launch of trace-route 63
Avaya VOIP Monitoring Manager 152

B

background tests 22
fixed interval 22
scheduled 22
backing up data 218
S8300D 218
backing up data files 216, 219
S8300 server 219
S8510 and duplicated servers 216
backup 207
creation 207
backup data files 226
restoring 226
backup files 227
types 227
backup history 221
view 221
backup logs 225
field descriptions 225
view 225
backup method 218
field descriptions 218
Backup Now 220
field descriptions 220
backup status 227
check 227
Backup web interface 45
batteries 309
preventive maintenance 309
bit rate 317
setting 317
BIU 235
replacing 235

C

C-LAN, VAL, and crossfire circuit packs 212, 213
disable S/FTP 213
enable S/FTP 212
cabling 177
DS1 connectors 177
call types 148
capabilities, system 32
carrier lead appearances 312
causes for 139
no dial tone 139
CEPT1 34
character code, 8-bit 35
characteristics, transmission 39
characters not displayed on IP telephone screen 341
resolution 341
check for a firewall 147
checking 227
backup status 227
checking network connectivity 142
MedPro and IP telephone 142
choppy voice 148
circuit packs 15, 232, 241, 242, 267
and electrostatic discharge (ESD) 15
DS1 CONV 232
isolating failures 267
packet-bus failures 242
replacing 232
requiring special procedures 232
reseating 232
TN572 232
TN573 232
TN750 232
using the packet bus 241
CLAN 130
signaling for multiple applications 130
CLAN board 127
checking for invalid board location 127
clearing 268
packet bus fault 268
CLI 46
defined 46
G450 and G430 commands 46
clipping 148
CMM 218
shutting down 218
CO-trunk-to-digital interface frequency response 39
codec 34
coder/decoder, analog-to-digital, see codec 34
codes 42
service 42
command history log 201–205
Abbreviated Dialing Button Programming log entries 204
CMS log entries 201
CTA, PSA, and TTI log entries 203
PMS log entries 202
Web activity log entries 205
command line interface 195
logged entries 195
Command Line Interface, see CLI 46
commands 256, 262
set tone-clock 262

to diagnose packet-bus problems 256
Communication Manager 57, 183
administer logging levels 183
maintenance features 57
Communication Manager application 62
initializing 62
Communication Manager restart log 194
Communication Manager time 178
complete shutdown failure 328
LED sequence 328
compromised system 208
reclaim 208
Conference, Transfer, and Call-Forwarding denial 38
configuring 266, 296
DS1 without smart jack 296
high- and critical-reliability systems 266
Connection Preserving Failover/Failback 73
connectivity 36, 164, 241
ISDN-BRI/packet bus 164
packet bus 241
rules 36
connectivity testing 310
TN760 310
correcting packet bus faults 238
tools 238
crackles 148
creating 207
backu[..... 207
CRON 187
crossfire circuit pack 214
disabling S/FTP 214
crossfire circuit packs 213
enable S/FTP 213

D

D-channel 32
protocol 32
data 32, 34
communications equipment, see DCE 32
service unit 34
terminal equipment 32
data-link layer, OSI 32
DC power 315
signaling leads 315
DCE 32
DCP 34
DCP Media Module 47, 49
demand tests 23
denial events 197
detecting 181, 263
circuit pack faults 263
system intrusion 181
diagnosing 139, 143, 149, 152
dropped calls 152
no-dial-tone problem 139
no-way talk path 143
one-way talk path 143
poor audio quality problem 149
Dialup modem access 45
via Maintenance Web Interface 45
digital 40, 42
port, insertion loss 40
to analog 40, 42
peak noise level 42
quantization distortion loss 40
Digital 34, 35
Multiplexed Interface (DMI) 35
Signal Level 1 (DS1) 34
disabling S/FTP 213, 214
C-LAN, VAL, and crossfire circuit packs 213
crossfire circuit pack 214
Disconnect Supervision 37
displaying 276
associated trunk group members 276
distortion 40
intermodulation 40
quantization loss 40
dropped call problems 152
resolution 152
DS0 Loop-Around Test Call 302
DS1 ..... 57, 177
cable connectors 177
DS1 CONV 176, 232
circuit packs 232
loopbacks 176
DS1 span 285, 286, 289
field descriptions 289
DSO frequency response 39
DSU, see Data Service Unit 34
DTE, see data terminal equipment 32
DTMR Test Call 302
duplicated series server 321
removing power 321
restoring power 321
duplication 170
of servers 170
spontaneous interchanges 170

E

E&M mode 312
ports wiring 312
E1/T1 Media Module 47, 49

tests ... 49
echo ... 41, 153
causes ... 153
return loss ... 41
EIA ... 39
Electronic Industries Association, see EIA ... 39
electrostatic discharge, ESD, circuit packs ... 15
enable/disable access protocols ... 215
enabling S/FTP ... 212, 213
C-LAN, VAL, and crossfire circuit packs ... 212
crossfire circuit packs ... 213
entering a new TN771D ... 250
standalone mode ... 250
entering installed TN771D ... 250
standalone mode ... 250
Enterprise Survivable Servers ... 63
traceroute command ... 63
ERL, see echo-return loss ... 41
error logs ... 21
error messages ... 341
resolution ... 341
errors ... 21, 24, 32
control ... 32
logs ... 21, 24
hardware ... 24
reporting, maintenance objects (MOs) ... 24
errors and denial events ... 278
causes ... 278
European conference of postal and Telecommunications rate 1, see CEPT1 ... 34
event report ... 118
expansion interface (EI) ... 175
manual loop-back procedure ... 175
expansion port networks ... 269
see port networks (PNs) ... 269
exporting ... 187
IP events logs ... 187
external ... 29
alarm leads ... 29

F

Facility Interface Code ... 43
Facility Test Calls ... 299
failed IP network region connections ... 134
failed ip-network-regions, testing ... 134
fan power filter ... 230
replacement ... 230
fault isolation ... 46
FCC ... 42
feature capacities ... 32
feature does not work ... 343
IP telephone ... 343
Federal Communications Commission, see FCC ... 42
fiber ... 171
fault-isolation procedure ... 171
fiber link faults ... 173
running tests for each fiber link's endpoints ... 173
fiber MUX ... 299
testing configurations ... 299
FIC, see Facility Interface Code ... 43
field descriptions ... 184
Logging Levels form page 1 ... 184
Logging Levels form page 2 ... 184
field replaceable components ... 46
filters ... 229
air filter ... 229
finding ... 280
assigned SBS extensions ... 280
firewall ... 192
logged entries ... 192
Firmware upgrades ... 45
flow control ... 32
frequency response ... 39
analog-to-analog ... 39
analog-to-digital ... 39

G

G430/G450 ... 215
SCP ... 215
G450 and G430 ... 46, 73
CLI commands ... 46
Standard Local Survivability ... 73
G450 and G430 gateways ... 326
restore power ... 326
G650 fan assembly ... 234
remove ... 234
G650 Serial Bus ... 269
fault detection and isolation ... 269
G650 server ... 234
replace fan ... 234
gateways ... 321
removing power ... 321
restoring power ... 321

H

H.248 link recovery ... 77
H.323 trunk groups ... 128
assigning to signaling groups ... 128
hairpinning ... 130
hairpinning and shuffling ... 135

using in different scenarios 135
hardware sanity 61
device 61
hmm Linux process 62
hot swap 47
S8300D caution 47
HTTP/web access log 194
details 194
HTTP/web SSL request log 193
details 193

I

iClarity 138
audio adjustments 138
impedance, setting 317
impedances 41
loop in 41
termination 41
inactive survivable server 327
manual shut down 327
initialization 61, 62
active server 62
arbiter module 61
Communication Manager application 62
hardware-sanity check 61
init process 61
server 61
standby server 62
watchdog process 61
initmap process 62
insertion loss 40
installing 236, 286
BIU or rectifier 236
loopback jack 286
installing loopback jack 286
without a Smart Jack 286
interchanges 262
commands 262
reset pnc interchange 262
reset system interchange 262
interface 34
physical 34
intermodulation distortion 40
intervening switching systems 36
IP connection status 131
station 131
trunk 131
IP events 195
logged entries 195
IP events logs 187
IP Network Region form 127
administering resource for a specified region 127
ip network region status 133
IP telephone 343
feature does not work 343
IP telephone, troubleshooting 136
IP telephones 137, 340, 344, 345
possible problems 340
power cycle 345
reset procedures 344
view LAN port address 137
IP telephones installation or administration not working 137
checking for System Parameters Customer Options 137
ISDN 32, 34, 57
BRI definition 34
D-channel treatment 32
PRI definition 34
ISDN-BRI 164
troubleshooting 164
ISDN-BRI and ASAI 159
problems 159
ISDN-PRI 156
troubleshooting 156
ISDN-PRI test call 165
synchronous method 165
ISDN-PRI test calls 166
asynchronous method 166
isolating 272
serial bus failure 272
isolating and correcting 237
packet-bus faults 237

J

jacks, network 43

L

lack of clarity with headset 342
causes 342
resolution 342
layers, of OSI model 34
and related protocols 34
LED sequence 327
shutdown failure 327
LEDs 15, 57, 106
legal notice 2
link recovery 77, 81, 83–85
feature interactions 84
link loss delay timer 81

mgc list 83
network fragmentation 85
primary search timer 83
total search timer 83
transition point 83
Linux 61, 62
commands 61
statapp 61
kernel 61
processes 62
hmm 62
scripts 61
rc 61
service startup 61
linux file transfer log 191
information 191
linux login/logout reboot log 191
contents 191
Linux time 178
Linux time and Communication Manager time 178
troubleshooting 178
Linx kernel debug messages 188
debug information 188
list ip interfaces clan 128
list testcalls 334
ATMS report 334
list trace station 152
lockout parameters 190
userlock 190
log entries 198, 207
common timestam[..... 198
details 198
without syslog header 207
logged logins 189
Logging Levels form page 1 184
field descriptions 184
Logging Levels form page 2 184
field descriptions 184
login lockout timer 189
logs 191–196
Communication Manager file synchronizations 194
Communication Manager restart log 194
hardware error and alarm events 196
HTTP/web access 194
HTTP/web server error 192
HTTP/web SSL request 193
linux file transfer 191
linux login/logout reboot 191
platform bash command history 195
platform command history 192
raw MST 196
SAT events 196
software events 196
system update/patch events 194
watchdog 191
loop input impedances 41
loopback jack 287, 290
administering 287
fault isolation procedures 290
loopback tests 176
fiber fault-isolation procedure 176
loopbacks 176
DS1 CONV 176
DS1 CONV tests 176
loss 40, 41
echo return 41
insertion 40
quantization distortion 40
single-frequency 41

M

mains power source 321
removing power 321
restoring power 321
maintaining 276
SBS signaling groups 276
maintenance 22, 46, 244, 309
arenas 46
background testing 22
packet bus 244
preventive 309
maintenance features 57
Communication Manager 57
maintenance objects (MOs) 21, 24
alarms 24
defined 21
maintenance objects, ... 24
error conditions 24
maintenance strategy 21
maintenance tasks 13
maintenance users 13
Maintenance Web Interface 45, 188
backup 45
check server status 45
current alarms 188
description 45
enabling remote access 45
restore 45
manually shutting down 327
inactive survivable server 327
MDF 196
Media Module 47, 49, 57

adding 47
DCP 49
E1/T1 47
hot swap 47
maintenance 47
removing 47
replacing 47
tests 57
voice announcement 49
media modules 106, 232
replacement 232
Media Modules 47, 49
Analog Media Module 49
analog trunk/telephone port board 47
DCP 47
E1/T1 49
MedPro 146, 148
common problems 148
verify allocated audio resources 146
MedPro and IP telephone 142
check network connectivity 142
MedPro resources unavailable 129
making a call 129
Message Tracker 196
mismatch of signals 36
monitoring 187
scheduled backup/restore 187
MST log 196
MTA 196
multicarrier cabinets 320
removing power 320
restoring power 320
Multimedia 44
multimedia interface 44
MMI 44

N

neon voltage 324, 325
adjust 324
adjustment 325
Neon voltage 324
network interface 291, 294, 295, 297, 298
dumb block 297
dumb block with repeater line to Fiber MUX 298
extended demarcation point 294
extended demarcation point when Smart Jack is accessible 295
network jacks 43
network recovery 73
timers 73
Final Cleanup Timer (FCT) 73
Link Loss Delay Timer (LLDT) 73
Primary Search Timer (PST) 73
Total Search Timer (TST) 73
Network Time Server 180
troubleshoot 180
no dial tone 341, 342
causes 341
resolution 342
no-dial-tone problem 139
resolution 139
no-way talk path 143, 147
diagnosing 143
verify whether MedPro can ping IP telephones 147
noise, peak level 42

O

one-way talk path 143, 147
diagnosing 143
verify whether MedPro can ping IP telephones 147
Open System Interconnect model 32, 34, 35
Layer 1 (physical layer) 32, 34
protocols 34
Layer 2 (data-link layer) 32, 35
protocols 35
operating system boot 187
messages log 187
OSI model, see Open System Interconnect model 32

P

packet bus 164, 238, 239, 241, 242, 244–246, 256, 257, 262
and circuit-pack failures 242
circuit packs 241
connectivity 241
correct general faults 246
definition 238
fault isolation 256
faults 239
in duplicated systems 262
ISDN-BRI connectivity 164
maintenance 244
maintenance software 245
reset pnc interchange 262
reset system interchange 262
set tone-clock 262
TDM-bus comparison 244
troubleshooting 257
packet bus fault 268
clear 268
packet bus fault correction 238, 251

standalone mode 251
tools 238
packet bus isolation fault 260
flowchart description 260
packet-bus fault 237, 239
correction 239
on-site maintenance 237
packet-bus faults 237, 239
isolate and correct 237
types 239
parts, field replaceable 46
PBX standard, RS-464A 39
PCD process 62
PCM-encoded analog signal 34, 36
peak noise level 42
performance 32, 41
echo-return loss 41
single-frequency return loss 41
physical layer, OSI 32
placing a call 306
test out-of service time slot 306
platform command history log 198
field descriptions 198
pops 148
port circuit packs 264
remove and reinsert 264
port networks (PNs) 269
troubleshooting packet bus 269
port-to-port insertion loss 40
power 28, 309, 320, 325
adding 325
distribution units 309
interruptions 28
power interruptions 28
removing 320
restoring 320
power cord 325
power interruption 340, 341
activating telephone 341
telephone server problems 340
power shutdown 322
shutting down the duplicated server 322
Shutting down the standby server 322
power source interruption 341
characters not displayed on IP telephone screen 341
preventive maintenance 309
batteries 309
PRI 34
private-line service codes 42
procedures 175
SNI/EI manual loop back 175
Process Manager (prc_mgr) 62
protocol analyzer 152
protocols 32, 34, 35
8-bit character code 35
ADU 34
analog 34
BRI 34
CEPT1 34
DCP 34
Digital Multiplexed Interface 35
in layers of OSI model 34
PRI 34
summary of states 35
system 32
voice-grade data 35
public key exchange 211

Q

quantization distortion loss 40

R

rc Linux script 61
rear panel connector 43
reclaiming 208
compromised system 208
rectifier 235
replacing 235
register stations 137
remote access 209
SSH and SFTP 209
removing 224, 234
G650 fan assembly 234
scheduled backup 224
removing and reinserting 264, 265, 271
multiple port circuit packs 271
PN control circuit packs 265
port circuit packs 264
REN, see ringer equivalency numbers 43
repairing packet bus faults 265
simplex control circuit packs 265
replacing 229–232, 234, 273
bus cabling and terminators 273
fan for G650 234
fan power filter 230
media modules 232
temperature sensor 231
variable-speed fans 229
reset 211, 262
dynamic host keys 211

SAT commands 262
reset pnc interchange 262
reset system interchange 262
resolving 152
dropped call problems 152
Restore web interface 45
restoring 226
backup data files 226
Restoring power 323
Duplicated servers 323
reusing 281
IPSI circuit packs 281
ring ping 324
ringer equivalency numbers 43
rootkit 181
RS-232 34
interface 34
RS-449 34
physical interface 34
RS-464A 39
rules, connectivity 36
run-on-standby processes 62

S

S8300 server 219
back up data files 219
S8300D 47, 218
data backup 218
disk parking 47
S8300D server 233
component maintenance 233
S8300D Server 47
hot swapping caution 47
shutdown 47
S8510 and duplicated servers 216
data backup 216
safety 14
caution, warning, danger 14
SAT 46
SAT commands 261
status port-network 261
SAT log 200
examples 200
SAT logs 199
field descriptions 199
SBS 275–277
extension status 277
no media processor issues 275
trunk service states 276
SBS calls 279
demand processor/ server interchanges 279
system resets 279
traffic measurements 279
upgrades 279
Schedule backup page 222
scheduled backup 222, 224
add or change 222
remove 224
SCP 215
security 181
system intrusion 181
selecting a slot 249
TN771D standalone mode 249
serial bus failure 272
isolation 272
server initialization 61
Duplicated server 61
servers 61, 169
duplicated, troubleshooting 169
software/firmware modules 61
service codes 42
set SAT commands 262
set tone-clock 262
setting 317, 324
bit rate 317
line impedance 317
neon voltage 324
SFRL, see single-frequency return loss 41
shadowing, between servers 62
shuffling 130
shutdown failure 327
LED sequence 327
shutting down 326
inactive survivable remote server 326
signaling leads, DC power 315
signaling type 316
summary 316
signals 36
mismatch 36
PCM-encoded analog 36
single-frequency return loss 41
SIP deskphones 345
documentation 345
smart jack 290, 292, 293
configurations 290
network interface 293
Network interface 292
SNI 175
manual loop-back procedure 175
software updates 192
logged entries 192
Software upgrades 45

specifications 32
spontaneous interchange of server 170
check standby server 170
spontaneous interchanges 169, 170
SSH and SFTP 210
symmetric algorithms 210
SSH and SFTP protocols 209
TN2312AP/BP (IPSI) 209
TN2501AP (VAL) 209
TN2602AP (Crossfire) 209
TN799DP (CLAN) 209
standalone mode display 255
field descriptions 255
Standard Local Survivability G450 and G430 73
startup Linux scripts 61
statapp Linux command 61
station 39
to CO trunk, frequency response 39
to digital interface, frequency response 39
to station, frequency response 39
status 61, 256, 261
Linux commands 61
statapp command 61
port-network 261
SAT commands 256
status commands 277
check parties in an SBS call 277
status station 152
status station command 277
status, ip network region 133
summary of protocol states 35
survivable remote server 326
shut down 326
switch 39
transmission characteristics 39
switch settings 315, 317
TN464 circuit pack 317
TN760 tie trunk 315
synchronization 32
syslog server 181, 182
administeration 182
log entries 181
system 32, 40
insertion loss 40
protocols 32
quantization distortion loss 40
specifications 32
system intrusion 181, 189, 192
firewall settings 192
logging root access 189
sniffer 181
warning signs 181
System Log page 197
display format options 197
system logs 119, 186
System Logs 194
select a viewpoint for log data 194
System Logs page 197
select event range options 197
System Tone Test Call 306

T

T1 285
talk path 142
one-way 142
problems 142
TDM bus 244, 304
packet bus comparison 244
time slots 304
TDM Bus Time Slot Test Call 303
TDM slot 304
test a time slot 304
technical specifications 32
telecommuter application 138
telephone does not ring 343
causes 343
resolution 343
temperature sensor 231
replacement 231
terminal 42
equipment port wiring 42
terminals and trunks usage 155
verification 155
terminating 273
serial bus at the end of a carrier 273
Terminating Trunk Transmission (TTT) test 315
termination impedances 41
test call 305
out-of-service time slot 305
test calls 299, 300, 302, 303, 306
DS0 loop around 302
DTMR 302
facility 299
system tone 306
TDM bus time slot 303
tone receiver 303
trunk 300
Test ISDN-TestCall response 167
field descriptions 167
test result 333
field descriptions 333
testcall trunk 60 332

results 332
testing 22, 23, 176
background 22
demand 23
fiber fault isolation 176
testing analog tie trunks 314
simplex mode 314
testing failed ip-network-regions 134
tests and audits 287
DS1 Span test 287
tie trunk 315
circuit pack option settings 315
time slots 304
TDM bus 304
timers 61
Watchdog 61
hardware timer 61
TN2302AP IP Media Processor does not work 127
causes 127
TN464 circuit pack 317
option settings 317
TN464E/F 318
option settings 318
TN572 circuit packs 232
TN573 circuit packs 232
TN750 circuit packs 232
TN760 circuit pack 315
option settings 315
TN760E 315
signaling formats 315
TN771D 246, 248, 249, 251, 255
exiting standalone mode 251
functions 246
special precaution 255
standalone mode 248, 249
TN771D packet bus 247
testing functions 247
TN771D standalone mode 248
hardware requirements 248
TN799DP board 127
checking for invalid board location 127
TN799DP boards 128
check for administered boards 128
TN799DP CLAN circuit pack does not work 127
causes 127
tones 307
system tone identification numbers 307
trace-route 63
traceroute 68
interpreting the Web interface logs 68
transmission 32, 39
characteristics 39
errors 32
stream 32
troubleshooting 13, 136, 158, 164, 165, 167, 169, 180, 257, 340
ASAI problems 164
duplicated servers 169
IP telephones 136, 340
ISDN- 158, 164, 165
BRI problems 164
PRI 158, 165
endpoints (wideband) 158
test-call problems 165
Network Time Server 180
outgoing ISDN-testcall command 167
packet bus 257
troubleshooting commands 110
trunk 36, 300
speed 36
test call 300
trunking 36
facilities 36
TTT, see Terminating Trunk Transmission 319
turning shuffling/hairpinning on 147

U

unregister H.323 endpoints 137
updating 284
software, firmware, and BIOS 284
UPS 28
UPS batteries 309
maintenance log 309
userlock 191
usage 191
userlock command 191
syntax 191

V

V.35, DTE-to-DCE interface 34
variable-speed fans 229
replacement 229
verify 146
call shuffling 146
verifying 146
voice audio reception from both IP telephones in a call 146
verifying consistent usage 151
802.1p QoS and IP DiffServ 151
verifying voice codec 151

G.729 151
viewing 221, 225
backup history 221
backup logs 225
voice announcement Media Module 49
tests 49
voice-grade data 35

W

Watchdog 61
processes 61
server-initialization process 61
watchdog log 191
contents 191
web interface 46
Web interface 185
accessing system logs 185
wiring 42
premises 42
terminal equipment ports 42