



Adding New Hardware for Avaya Servers and Branch Gateways

03-300684
Issue 5
July 2012

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

Disclaimer

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: <http://support.avaya.com>. 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 IECCE 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 Laserlaitte
- 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:

A. 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

B. 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 matériel est conforme aux spécifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Européenne) 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。

Downloading documentation

For the most current versions of documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support Web site: <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 Web site: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

About this document	11
Overview	11
Audience	11
Using this document	11
Conventions	11
General	12
Physical dimensions	12
Terminology	12
Typography	12
Commands	13
Keys	13
User input	13
System output and field names	14
Downloading this book and updates from the Web	14
Downloading this document	14
Safety labels and security alert labels	15
Related resources	15
Support	15
Technical assistance	16
Within the US	16
International	16
Trademarks	16
Sending comments	16
Chapter 1: Introduction	17
Chapter 2: IP connectivity hardware	19
Installing the circuit packs	19
Installing and administering IP connectivity hardware	20
TN799DP Control LAN	20
Checking your shipment	21
Installing a TN799DP C-LAN	21
Installing the cables connected to the C-LAN circuit pack	22
Installing the circuit packs	23
Administering the TN799DP	23
Testing the external connection to the LAN	24
TN2302AP IP Media Processor	25
Checking your shipment	26
Installing a TN2302AP IP Media Processor	26

Contents

Installing the cables for the IP Media Processor circuit pack	27
Installing the circuit packs	28
Administering the IP Media Processor	28
Testing the external connection to the LAN	29
Verifying active call status	29
TN2501AP Voice announcements over LAN (VAL)	29
Installing a TN2501AP VAL	30
Testing the external connection to the LAN	33
TN2602AP IP Media Resource 320	33
Installing the TN2602AP Media Resource 320	34
Checking your shipment	35
Installing a TN2602AP IP Media Resource 320.	36
Installing the cables	36
Installing the circuit packs	37
Verifying installation and voice channels	38
Administering the TN2602AP circuit pack	38
Testing the external connection to the LAN	40
Verifying active call status	40
Testing the circuit pack	40
Upgrading firmware (if necessary)	40
Firmware upgrades	40
Replacing the I/O cables	41
Chapter 3: Trunks and lines	45
List of analog and digital trunk and line circuit packs	45
Adding TN464HP/TN2464CP with echo cancellation	46
Adding CO, FX, WATS, and PCOL	48
Adding DID trunks	49
Adding Analog Tie trunks	49
Adding digital DS1 Tie trunks and OPS	51
Adding TTC Japan 2-Mbit trunk	51
Adding CAMA/E911 trunk	52
Installing the circuit pack	53
Adding the trunks	53
Changing the feature access code	54
Changing the ARS digit analysis	54
Changing the route patterns	55
Changing the CAMA numbering and class of restriction	55
Adding ISDN—PRI	56

North American	56
International	56
Adding circuit packs.	57
Connecting cables.	57
Administering the circuit pack	57
Resolving alarms	57
Saving translations	58
Chapter 4: Port networks	59
Installing a G650 Media Gateway	59
Installing the IPSI circuit pack	59
Assigning IP addresses to the IPSI circuit packs	60
Clearing the ARP cache on the laptop	61
Logging in to the IPSI	61
Setting the control interface	62
Setting the VLAN and diffserv parameters.	63
Administering the port network	63
Adding IPSI translations to Communication Manager	64
Setting IPSI duplication for duplicated control network only.	64
Setting alarm activation level	64
Verifying IPSI translations	65
Verifying IPSI connectivity	65
Installing additional circuit packs	65
Chapter 5: Adjuncts and peripherals.	67
Terminal server installation	67
Installing and administering the terminal server	68
Distance limits	69
Cable connection diagram	69
Making the connections.	70
Administering the IOLAN+	71
Potential failure scenarios and repair actions	78
Administering IP node names	78
Administering IP services.	79
Call detail recording	80
Connecting CDR Equipment	80
Administering CDR data collection	80
Administering CDR parameters	81
Testing the switch-to-adjunct link	82

Contents

Reliable Data Transport Tool package	82
Contents of the RDTT	82
Downloading RDTT	83
Installing RDTT	83
Administering RDTT	83
Related topics	84
Wideband endpoints.	84
Nonsignaling configuration	84
Signaling configuration	85
Multimedia call handling	87
Connecting the endpoints.	88
Administering the system	88
Administering the endpoints	89
Administering one number complex	89
Expansion services module.	89
ESM installation	90
Administration	90
Place test call	91
Troubleshooting	92
Printers	92
Connecting printers using TCP/IP	92
Task list.	92
Administering adjunct parameters	93
Using the downloadable reliable session-layer protocol (RSP) tool	93
DS1/T1 CPE loopback jack	94
Installing a loopback jack	94
With a smart jack.	94
Without a smart jack.	95
Administering the loopback jack	96
Loopback testing with a smart jack	96
Testing the DS1 span from the ICSU to the loopback jack	96
Restoring DS1 administration.	102
Releasing the DS1 circuit pack	102
Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer (MUX)	102
Testing the DS1 span from the loopback jack to the smart jack	103
Testing a loopback jack without a smart jack	106
Configurations using fiber multiplexers	109
ISDN converters and adapters	110
Converters for single-carrier cabinets	111

PRI-to-DASS and PRI-to-DPNSS converters	111
PRI-to-BRI converter.	111
Converters for multicarrier cabinets	113
PRI-to-DASS and PRI-to-DPNSS converters	113
PRI-to-BRI converter.	114
Busy tone disconnect equipment for non-U.S. installations	114
909A/B universal coupler	115
Malicious call trace	119
Music-on-hold	120
Registered music source	121
Nonregistered music source	121
Unregistered music source on a G700 or G350 Branch Gateway	123
Registered music source on a G700 or G350 Branch Gateway.	125
Paging and announcement equipment.	126
Loudspeaker paging.	127
Loudspeaker paging without paging adapter	127
Loudspeaker paging access without universal coupler	128
Loudspeaker paging with universal coupler.	129
ESPA radio paging.	130
External ringing	130
Queue warning indicator	131
Loudspeaker paging.	131
Adjunct information sources	132
Call Management System	132
Avaya Aura Messaging	132
ASAI and DEFINITY LAN Gateway	133
Avaya Interactive Response	133
Avaya Extension to Cellular.	133
Property Management Systems	133
DEFINITY Wireless Business System	133
Index	135

Contents

About this document

Overview

This document provides procedures to add hardware to an existing server configuration.

This document does not contain information on all the adjuncts and peripheral equipment that an Avaya server supports. For more information, see [Related resources](#) on page 15.

Audience

This document is for the following audiences:

- Technical support representatives
- Authorized Business Partners

Using this document

Use this document as a guide to install and administer hardware. For more information about a particular task, see the index or table of contents to locate the page number where the information is described.

This document includes the following information:

- [IP connectivity hardware](#) on page 19
- [Trunks and lines](#) on page 45
- [Port networks](#) on page 59
- [Adjuncts and peripherals](#) on page 67

Conventions

This section describes the conventions that we use in this book.

General

This document includes commands and screens from the latest version of Avaya Aura® Communication Manager and refer to the most current document of Communication Manager.

Physical dimensions

All physical dimensions are in English units followed by metric units in parentheses. Wire gauge measurements are in AWG followed by the diameter in millimeters in parentheses.

Terminology

The following terminology is used in this document:

- *Configuration* is a general term that encompasses all references to an Avaya server with branch gateways running Communication Manager.
 - *Cabinet* refers to a stack of branch gateways, such as the G650, that are TDM-cabled together. A cabinet is the same as a port network.
 - *UUCSS* refers to a circuit pack address in cabinet-carrier-slot order.
 - *Telephone* and *voice terminal* have the same meaning.
 - *ASAI* is synonymous with the newer CallVisor ASAI.
-

Typography

This section describes the typographical conventions for the following:

- Commands
- Keys
- User input
- System output
- Field names

Commands

Commands are in **bold monospaced** type.

Example

Type **change-switch-time-zone** and press **Enter**.

Command variables are in **bold *italic monospaced*** type.

Example

Type **change machine *machine_name***, where *machine_name* is the name of the call delivery machine.

Command options are in **bold** type inside square brackets.

Example

Type **copybcf [-F34]**.

Keys

The names of keys are in **bold** type.

Example

Use the **Down Arrow** key to scroll through the fields.

When you must press and hold a key and then press a second or third key, separate the names of the keys with a plus sign (+).

Example

Press **ALT+D**.

When you must press two or more keys in sequence, separate the names of the keys with a space.

Example

Press **Escape J**.

When you must press a function key, provide the function of the key in parentheses after the name of the key.

Example

Press **F3 (Save)**.

User input

User input is in **bold** type. User input includes when you must type the input, select the input from a menu, or click a button or similar element on a screen or a Web page.

Examples

- Press **Enter**.
- On the **File** menu, click **Save**.
- On the **Network Gateway** page, click **Configure > Hardware**.

System output and field names

System output on the screen is in **bold** type.

Example

- The system displays the following message:

The installation is in progress.

Field names on the screen are in **bold** type.

Example

- Type **y** in the **Message Transfer?** field.

Downloading this book and updates from the Web

You can download the latest version of this document from the Avaya Support Web site <http://support.avaya.com>. You must have access to the Internet and a copy of Adobe Reader installed on your personal computer.

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

Downloading this document

To download the latest version of this document:

1. Access the Avaya Support Web site at <http://support.avaya.com>.
2. In the **SEARCH AVAYA SUPPORT** text box, type the document number 555-245-112 and click the arrow button.
3. In the resulting list, locate the latest version of this document.
4. Click the document title to view the document in PDF Format.

Safety labels 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 document 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, including ESD damage to electronic components.

**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 access to a server or use of a telecommunications system.

Related resources

For more information, see *Avaya Communication Manager, Branch Gateways and Servers* (03-300151).

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at <http://support.avaya.com>, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya Technical Consulting and System Support (TC-SS) at 1-800-225-7585.
- Maintenance and warranty technical support, call the Avaya National Customer Care Support Line at 1-800-242-2121.
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353.

International

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

Trademarks

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

Sending comments

Avaya welcomes your comments on this book. You can send your comments to:
infodev@avaya.com.

In comment, mention the name and number of this document, *Adding New Hardware for Avaya Servers and Branch Gateways*, 03-300684.

Chapter 1: Introduction

This book only provides the information for adding the circuit packs to G650 Media Gateway. This book provides information on adding hardware to an existing Server configuration. Hardware includes circuit packs for existing branch gateways, new branch gateways that make up new port networks, and adjunct or peripheral equipment.

This book includes the following information:

- [IP connectivity hardware](#) on page 19
 - [Installing the circuit packs](#) on page 19
 - [Installing and administering IP connectivity hardware](#) on page 20
- [Trunks and lines](#) on page 45
- [Port networks](#) on page 59
- [Adjuncts and peripherals](#) on page 67

Chapter 2: IP connectivity hardware

This chapter provides procedures for:

- [Installing the circuit packs](#) on page 19
- [Installing and administering IP connectivity hardware](#) on page 20.

Note:

If a circuit pack requires a right-to-use fee for a particular feature, you must have a license file to enable the feature.

When installing additional features or equipment, you might need to install additional circuit packs. Use the following general procedure when adding features or equipment that require adding circuit packs.

Note:

Duplicated servers: For a duplicated server, you must log in to the *active* server to access SAT commands. You can use the Avaya Site Administration (ASA), the System Access Terminal (SAT) program, or the Native Configuration Manager interface.

1. Log in to the server using a services login.
2. Install the TN circuit pack in the gateway.
3. Perform the minimally required administration so that Communication Manager recognizes the circuit pack.
4. Log off the server after you complete the addition and any required administration.

For more information about further administering circuit packs and other equipment, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Installing the circuit packs



CAUTION:

When adding or replacing any hardware and associated cables and adapters, be sure to ground yourself against electrostatic discharge (ESD). Wear a grounded wrist strap.

Note:

Circuit packs are hot-swappable, so you do not need to turn off the power to the carrier or branch gateway to install them.

Note:

To properly seat a circuit pack, push firmly on the front of the faceplate until the latch reaches the bottom rail of the carrier. Then close the latch until latch is fully engaged.

To Install a TN circuit pack:

1. Insert the circuit pack into any port slot. If the circuit pack was assigned a slot location, place the circuit pack in the assigned slot.
2. To verify that the system recognizes the newly installed circuit packs, type **list configuration all** and press **Enter**.

Installing and administering IP connectivity hardware

Several port circuit packs are used specifically for IP connectivity. This section provides information on installing the following circuit packs:

- [TN799DP Control LAN](#) on page 20
- [TN2302AP IP Media Processor](#) on page 25
- [TN2501AP Voice announcements over LAN \(VAL\)](#) on page 29
- [TN2602AP IP Media Resource 320](#) on page 33

TN799DP Control LAN

The TN799DP Control LAN circuit pack provides:

- A connection for the signaling (telephone) network to your data network for IP telephones.
- A source board for downloading firmware to circuit packs having the P designation.
- An IP interface for adjuncts such as CM Messaging.
- An IP interface for DCS connection with another Avaya configuration.

For more information, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Check the firmware vintage and upgrade availability for the TN799DP circuit pack on the Avaya Support Web site: <http://support.avaya.com>.

The following sections describe the process of installing the circuit pack:

- [Checking your shipment](#) on page 21
- [Installing a TN799DP C-LAN](#) on page 21

- [Installing the cables connected to the C-LAN circuit pack](#) on page 22
- [Installing the circuit packs](#) on page 23
- [Administering the TN799DP](#) on page 23
- [Testing the external connection to the LAN](#) on page 24

Checking your shipment

When the order arrives at your site, check the contents. See [Table 1: Required hardware](#) on page 21).

1. Inspect the shipping carton for damage before opening the box. If the box is damaged, *do not open* the carton. Inform the shipping company, and ask for instructions on filing a claim.
2. If the box is undamaged, check the contents against the packing slip. Check the condition of each component, and note any damage or shortages on the packing slip. The carton should contain the items in [Table 1: Required hardware](#) for each TN799DP C-LAN circuit pack ordered.
3. Read and follow any directions inserted into the package by the factory.

Table 1: Required hardware

Description	Quantity
TN799DP Control LAN circuit pack	1 or more
IP Media Processor adapter ¹	1/C-LAN

¹The adapter has an amphenol connector on one side and an RJ45 connector on the other for connecting to the network at 100 Mbps.

Installing a TN799DP C-LAN

Ensure that the following equipment is on site:

- An unoccupied port slot for the TN799DP.
- A 10 or 100 BaseT Ethernet connection for LAN with the TN799DP.
- One or more valid, unused IP addresses on the network, one for each TN799DP C-LAN, that you can assign to the C-LAN circuit pack. You also need the subnet mask and default gateway.
- An Ethernet adapter for each TN799DP.
- A CAT5 (100 Mbps) cable with a DW8 connector on each end.

Installing the cables connected to the C-LAN circuit pack

Perform the following steps:

1. Determine the port slots into which you will place the TN799DP C-LAN circuit packs.

From the rear of the branch gateway:

Note:

To install the TN799DP into an old carrier or cabinet, replace the WP cables that connect the backplane to the rear connector panel by Twisted Pair I/O cables to handle the 100-Mbps speed. For information on replacing the wires, see [Replacing the I/O cables](#) on page 41.

2. From the rear of the branch gateway, connect the Ethernet adapter to the Amphenol connector corresponding to each TN799DP slot. See [Figure 1: Cable connection for C-LAN](#) on page 22. For a pinout of TN799DP, see [Table 2: TN799DP pinout](#) on page 23.
3. Connect one end of each CAT5 cable to each Ethernet adapter.
4. Install the other end of this cable from the branch gateway to the network through a hub or 110 (purple) wall field as required.

Figure 1: Cable connection for C-LAN

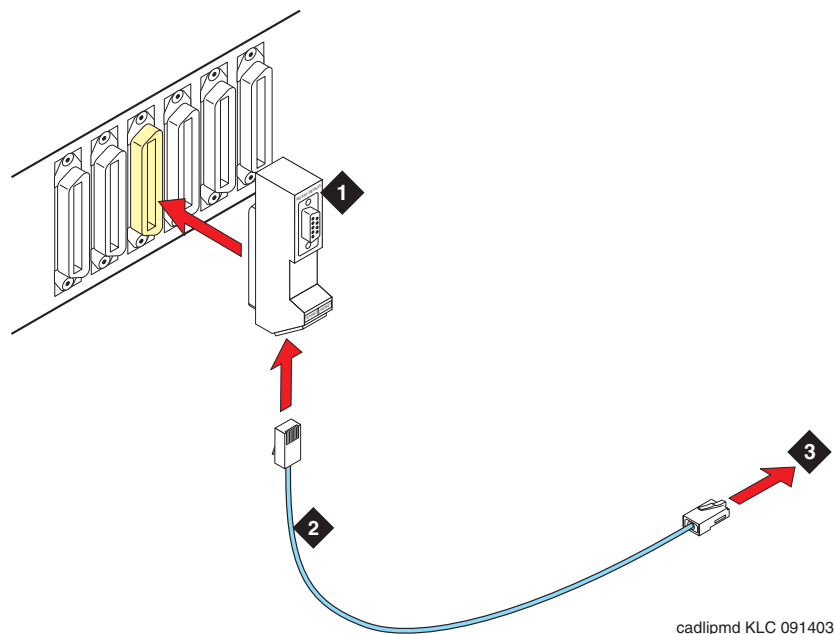


Figure notes:

- | | |
|-----------------------------------|--------------------|
| 1. Ethernet adapter | 3. To your network |
| 2. CAT5 cable with DW8 connectors | |

Table 2: TN799DP pinout

Backplane pin	25-Pair wire color	Lead name	Peripheral connector pin
103	White/Orange	TD+	27
003	Orange/White	TD-	2
104	White/Green	RD+	28
004	Green/White	RD-	3

Installing the circuit packs



CAUTION:

When adding or replacing any hardware, be sure to ground yourself against electrostatic discharge (ESD) by wearing a grounded wrist strap.

Note:

The TN799DP circuit packs are hot-swappable, so you do not need to turn off the gateway to install them.

Note:

Set the port on your Ethernet switch to 100 speed and full duplicated server.

To install the circuit pack:

1. Insert the TN799DP circuit packs into the port slots identified earlier.
2. Push firmly on the front of the faceplate until the latch reaches the bottom rail of the carrier to properly seat the circuit pack.
3. Close the latch until latch is fully engaged.

Administering the TN799DP

Use a terminal emulation application for the administration.

Note:

The customer or design team provides the actual names, IP addresses, subnet masks, and gateway addresses.

1. Log in as **craft**.
2. Type **list configuration all** and press **Enter** to verify that Communication Manager recognizes the TN799DP circuit packs.
3. Type **add node-name ip** and press **Enter**.

4. Type the node names and IP addresses for each TN799DP C-LAN circuit pack.
5. Type **display circuit-pack cabinetnumber**, where *cabinetnumber* is the cabinet where the circuit packs reside to verify that the TN799DP shows up in the **Code** column. Press **Enter**.
6. Type **add ip-interface *UU*CS**, where *UU* is the cabinet, *C* is the carrier, and *SS* is the slot location of the TN799DP C-LAN circuit pack. Press **Enter**.
7. Type the following information:
 - The **Type**, **Slot**, **IP Address**, and **Code/Suffix** fields are populated automatically.
 - In the **Node Name** field, type the same node name entered on the **Node Name** screen.
 - In the **Subnet Mask** field, use the default setting unless you are given a different subnet mask.
 - In the **Gateway Address** field, use the address you are given or leave blank.
 - Set the **Enable Ethernet Port** field to **y**.
 - Set the **Net Region** field to **1** unless you are given a different number.
 - Set **VLAN** field to **n**.
8. Press **Enter** to save the information and effect the new settings.
9. Type **add data-module next** and press **Enter**.
10. Set the **Type** field to **ethernet**.
11. Set the **Port** field to correspond to the circuit pack location.

The port number (final two digits) is always 17 for the TN799DP circuit pack.
12. Set the **Link** field to an unassigned or next-available link number.
13. Set the **Network uses 1's for Broadcast Address?** field according to the your network requirements.
14. Type a unique name in the **Name** field.
15. Press **Enter** to save your changes.

For more information on these administration steps and for the steps to administer endpoints, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Testing the external connection to the LAN

To test the external IP connections, ping the gateway and a known computer connected to the network. If everything is configured correctly, you have a successful ping. If you cannot ping, verify the IP-address information and check the connectivity, including the cabling.

To test the external IP connections, ping a computer on the same subnet, the gateway, and a computer beyond the gateway. If everything is configured correctly, the **Result** column on the

Ping Results screen reads **pass**. If it reads **abort**, verify the IP-address information and check the connectivity, including the cabling.

1. Type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of a computer on the same subnet and *UUCSS* is the cabinet, carrier, and slot location of the TN799DP C-LAN circuit pack that is used to ping. Press **Enter**.
2. If the **Ping Results** screen reads pass at Step 1 passes, type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of your gateway and *UUCSS* is the cabinet, carrier, and slot location. Press **Enter**.
3. If the **Ping Results** screen reads pass at Step 2 passes, type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of a computer beyond the gateway and *UUCSS* is the cabinet, carrier, and slot location. Press **Enter**.

The TN799DP C-LAN circuit pack is now installed in the branch gateway and connected to the IP network.

TN2302AP IP Media Processor

The TN2302AP IP Media Processor circuit pack provides an interface between your IP network and Avaya branch gateways. This interface transports voice and FAX between the branch gateways and IP devices, such as H.323 V2 compliant endpoints and other Avaya telephone systems. Each TN2302AP can support 32 to 64 voice channels, depending on the codecs used.

Note:

The P suffix indicates that the circuit pack is firmware-downloadable.

Check the firmware vintage and upgrade availability for the TN2302AP circuit pack on the Avaya Support Web site: <http://support.avaya.com>.

The following sections describe the process of installing the circuit pack:

- [Checking your shipment](#) on page 26
- [Installing a TN2302AP IP Media Processor](#) on page 26
- [Installing the cables for the IP Media Processor circuit pack](#) on page 27
- [Installing the circuit packs](#) on page 28
- [Administering the IP Media Processor](#) on page 28
- [Testing the external connection to the LAN](#) on page 29
- [Verifying active call status](#) on page 29

For further administration, see the *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Checking your shipment

When the order arrives at your site, check the contents. See [Table 3: Required Hardware](#) on page 26).

1. Inspect the shipping carton for damage before opening the box. If the box is damaged, *do not open the carton*. Inform the shipping company, and ask for instructions on filing a claim.
2. If the box is undamaged, check the contents against the packing slip. Check the condition of each component, and note any damage or shortages on the packing slip. The carton should contain the items in [Table 3: Required Hardware](#) for each TN2302AP IP Media Processor circuit pack ordered.
3. Read and follow any directions inserted into the package by the factory.

Table 3: Required Hardware

Description	Quantity
TN2302AP IP Media Processor (MedPro)	1 or more
TN2302AP Amphenol Adapter ¹	1/MedPro

¹The adapter has an amphenol connector on one side and an RJ45 connector on the other for connecting to the network. See [TN2302AP Amphenol Adapter](#) on page 27.

Note:

You must provide one CAT5 or better cable for each TN2302AP.

Installing a TN2302AP IP Media Processor

The TN2302AP consumes 16 watts of power and the power budget is 15 watts per slot. Do not fill every available slot in the gateways with these circuit packs. Use the following guidelines:

- G650—5 per media gateway

Ensure the following equipment is on site before your shipment arrives:

- An unoccupied port slot in the branch gateway for each TN2302AP IP Media Processor
- A 10 BaseT or 10/100 BaseT Ethernet connection into your local area network (LAN)
- One or more valid, unused IP addresses on the network that can be assigned to the IP Media Processor server. You also need the subnet mask and default gateway.

Note:

Obtain this information from the project manager or network administrator.

In addition to the TN2302AP IP Media Processor, you also must install and administer a TN799CP C-LAN circuit pack. For C-LAN installation and administration, see [TN799DP Control LAN](#) on page 20.

Installing the cables for the IP Media Processor circuit pack

Perform the following steps:

1. Determine the port slots into which you will place the TN2302AP IP Media Processor circuit packs.

From the rear of the branch gateway:

Note:

To install the TN2302AP into an old carrier or cabinet, replace the WP cables that connect the backplane to the rear connector panel by Twisted Pair I/O cables to handle the 100-Mbps speed. For information on replacing the wires, see [Replacing the I/O cables](#) on page 41.

2. Connect the amphenol connector on the adapter to the Amphenol connector corresponding to each TN2302AP slot. See [Figure 2: TN2302AP Amphenol Adapter](#) on page 27.

Figure 2: TN2302AP Amphenol Adapter

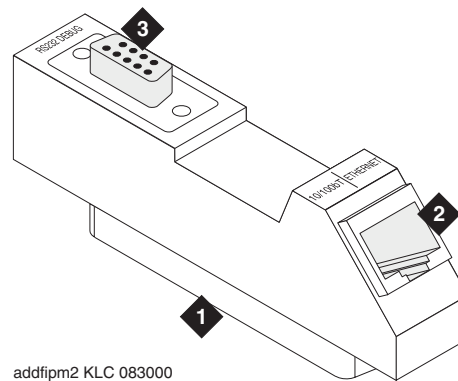


Figure notes:

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. Amphenol connector to backplane connector corresponding to TN2302AP slot | <ol style="list-style-type: none"> 2. RJ45 LAN cable connection <ul style="list-style-type: none"> ● 10 Mbps uses CAT3 cable ● 100 Mbps uses CAT5 cable 3. 9-pin connector for maintenance |
|---|---|

Note:

You need a CAT5 or better cable for 100-Mbps operation.

3. Connect the network cables to the ETHERNET connector on the TN2302AP backplane adapters.

Installing the circuit packs



CAUTION:

When adding or replacing any hardware, be sure to ground yourself against electrostatic discharge (ESD) by wearing a grounded wrist strap.

Note:

The TN2302AP circuit packs are hot-swappable, so you do not need to turn off the branch gateway to install them.

Note:

To properly seat the circuit pack, push firmly on the front of the faceplate until the latch reaches the bottom rail of the carrier. Then close the latch until latch is fully engaged.

Note:

Set the port on your Ethernet switch to 100 speed and full duplicated server.

To install the circuit pack.

1. Insert the TN2302AP IP Media Processor into the port slot you reserved for TN2302AP IP Media Processor and seat the TN2302AP IP Media Processor properly.

When you plug in the TN2302AP IP Media Processor, the circuit pack starts to boot. The RED LED stays on until you assign an IP address to the circuit pack.

Administering the IP Media Processor

Use a terminal emulation application for the administration.

1. Log in as **craft**.
2. Type **list configuration all** and press **Enter** to verify that Communication Manager recognizes the TN2302AP circuit packs.
3. Type **add node-names** and press **Enter**.
4. On page 2, type the node names and IP addresses for the TN2302AP.
5. Type **display circuit-pack** and press **Enter**. Verify that the **Code** column displays TN2302AP.
6. Type **add ip-interface VUCSS** and press **Enter**, where **VUCSS** is the cabinet, carrier, and slot location.
7. Type the following information:
 - The **Type**, **Slot**, **IP Address**, and **Code/Suffix** fields are populated automatically.
 - In the **Node Name** field, type the same node name entered on the **Node Name** screen.
 - In the **Subnet Mask** field, use the default setting unless you are given a different subnet mask.

- In the **Gateway Address** field, use the address you are given or leave blank.
 - Set the **Enable Ethernet Port** field to **y**.
 - Set the **Net Region** field to **1** unless you are given a different number.
 - Set **VLAN** to **n**.
8. Press **Enter** to save the information and effect the new settings.

Testing the external connection to the LAN

To test the external IP connections, ping a computer on the same subnet, the gateway, and a computer beyond the gateway. If everything is configured correctly, the **Result** column on the **Ping Results** screen reads **pass**. If it reads **abort**, verify the IP-address information and check the connectivity, including the cabling.

1. Type `ping ip-address ipaddress board UUCSS` and press **Enter**, where *ipaddress* is the IP address of a computer on the same subnet and *UUCSS* is the cabinet, carrier, and slot location of the TN2302AP IP Media Processor.
2. If the **Ping Results** screen reads pass at Step 1, type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of your gateway and *UUCSS* is the cabinet, carrier, and slot location. Press **Enter**.
3. If the **Ping Results** screen reads pass at Step 2 passes, type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of a computer beyond the gateway and *UUCSS* is the cabinet, carrier, and slot location. Press **Enter**.

The TN2302AP IP Media Processor circuit pack is now installed in the branch gateway and connected to the IP network.

Verifying active call status

To verify that calls are being processed:

1. Type `status media processor board UUCSS`.
2. Look at the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether calls are being processed.

For more information on these administration steps and for the steps to administer endpoints, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

TN2501AP Voice announcements over LAN (VAL)

The TN2501AP voice announcements over LAN (VAL) circuit pack is an integrated announcement circuit pack that uses *.wav files for announcements and plays the files over the TDM bus. TN2501AP VAL has a storage capacity of up to 1 hour of announcement.

Installing a TN2501AP VAL

Note:

The P suffix indicates that the circuit pack is firmware-downloadable.

Note:

To install a TN2501AP, make sure that the system is enabled for TN2501AP (VAL) circuit packs. If the **Maximum VAL boards** field on the **System Parameters Customer Options** screen is set to **0**, then you must obtain and install a new license file before you can install the card.

Check the firmware vintage and upgrade availability for the TN2501AP circuit pack on the Avaya Support Web site: <http://support.avaya.com>.

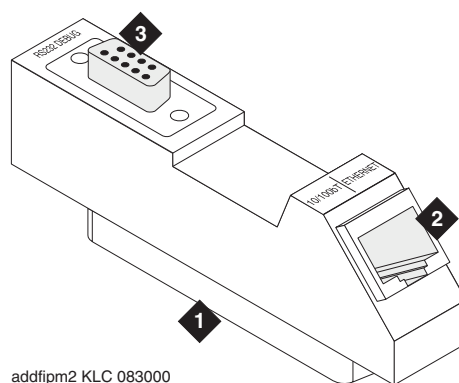
The following sections describe the process of installing the circuit pack:

- [Verifying the required hardware](#) on page 30
- [Installing the circuit packs](#) on page 31
- [Administering the TN2501AP](#) on page 32

Verifying the required hardware

Make sure that you have the required hardware:

- TN2501AP VAL circuit pack (108772583).
- 10/100BaseT backplane adapter. For example, 848525887, that is the same one used for the IP Media Processor. See [Figure 3: Backplane adapter](#) on page 31.
- Tight-twisted I/O cable kit (700234032) to install in old carriers or cabinets with WP cables.
- LAN cable with RJ45 connectors supplied by the customer.

Figure 3: Backplane adapter**Figure notes:**

- | | |
|---|---|
| <p>1. Amphenol connector to backplane connector corresponding to TN2501AP slot</p> | <p>2. RJ45 LAN cable connection</p> <ul style="list-style-type: none"> ● 10 Mbps uses CAT3 cable ● 100 Mbps uses CAT5 cable <p>3. This connector is not used for VAL.</p> |
|---|---|

Installing the circuit packs**WARNING:**

To prevent electrostatic discharge (ESD), wear a grounding strap while handling the circuit pack.

1. Insert the circuit pack into any port slot and close the latch securely.

At first, the red and green LEDs are on steady, then the green LED flashes. If there are announcements on the circuit pack, the amber LED flashes while the announcements are copied from FLASH to RAM. After about 3-5 minutes, the top 3 LEDs switch off, although the time is longer if there are announcements already recorded on the circuit pack.

Note:

If the TN2501AP circuit packs are at the Communication Manager limit and you insert a VAL circuit pack, the red LED on that circuit pack stays on, indicating that Communication Manager does not accept the VAL circuit pack.

Note:

To install the TN2501AP in an old carrier or cabinet, you must replace the WP cables, which connect the backplane to the rear connector panel, with Twisted Pair I/O cables to handle the 100-Mbps speed. For information on replacing the wires, see [Replacing the I/O cables](#) on page 41.

2. Connect the backplane adapter to the Amphenol connector on the back of the branch gateway corresponding to the TN2501AP circuit pack slot.
3. Connect the LAN CAT5 cable to the RJ45 connector on the backplane adapter.

Administering the TN2501AP

After you install the hardware, administer and test the installation to support an FTP session.

Use a terminal emulation application or Avaya Site Administration for this administration.

1. Type `list configuration board board-location` and press **Enter**.

The system displays the System Configuration report. Use this report to ensure that Communication Manager recognizes the TN2501AP circuit pack after TN2501AP circuit pack is latched to the carrier slot.

2. Verify the following field values:

- **Board Type** displays **VAL-ANNOUNCEMENT**
- **Code** displays **TN2501AP**

3. Type `add node-names ip` and press **Enter**.

4. In the **Name** field, type a unique name.

Communication Manager accepts the unique name, and you do not have to match the node name on your network.

5. In the **IP Address** field, type the **IP Address**.

Obtain this information from the project manager or your network administrator.

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

7. Type `add ip-interface UUCSS` and press **Enter**, where *UUCSS* is the cabinet, carrier, and slot location.

8. Type the following information:

- The **Type**, **Slot**, **IP Address**, and **Code/Suffix** fields are populated automatically.
- In the **Node Name** field, type the same node name entered on the **Node Name** screen.
- In the **Subnet Mask** field, use the default setting unless you have a different subnet mask.
- In the **Gateway Address** field, use the address you are given or leave blank.
- Set the **Enable Ethernet Port** field to **y**.
- Set the **Net Region** field to **1** unless you are given a different number.
- Set **VLAN** to **n**.

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

10. Type `add data-module extension` and press **Enter**.

11. Set the **Type** field to **ethernet**.

12. Set the **Port** field to correspond to the circuit pack location.
The final two digits of the port number are always **33** for the TN2501AP circuit pack.
13. Set the **Link** field to an unassigned or the next available link number.
14. Set the **Network uses 1's for Broadcast Address?** field according to your network requirements.
15. In the **Name** field, type a unique name.
16. Press **Enter** to save the changes.
17. Type `add ip-route` and press **Enter**.
18. Administer IP routes to the TN2501AP circuit pack.
19. Press **Enter** to save the changes.

Testing the external connection to the LAN

To test the connection to the LAN.

1. Click **Start > Run** to open the Run dialog box.
2. Type `command` and press **Enter** to open an MS-DOS command window.
3. Type `ping ipaddress`, where *ipaddress* is a known computer on the network, and press **Enter** to verify connectivity.
4. To test the new IP connections that you administered, type `status link`.

The system displays the status of each new IP connection.

TN2602AP IP Media Resource 320

The TN2602AP IP Media Resource 320 provides high-capacity voice over Internet protocol (VoIP) audio access to the switch for local stations and outside trunks. The IP Media Resource 320 provides audio processing for the following types of calls:

- TDM-to-IP and IP-to-TDM: For example, a call from a 4602 IP telephone to a 6402 DCP telephone.
- IP-to-IP: For example, a non shuffled conference call.

The TN2602AP IP Media Resource 320 circuit pack has 320 voice channels. Each port network can support only two TN2602AP circuit packs.

The two TN2602AP circuit packs that you install in a single port network act as load balancers. The TN2602AP circuit pack is also compatible with the TN2302 and TN802B IP Media Processor circuit packs and can share load balancing with these circuit packs. A variety of factors might affect the actual capacity, including the codec used for a call and fax support.

Note:

When two TN2602AP circuit packs, each with 320 voice channels, are used for load balancing within a port network, the total number of voice channels available totals 484 because 484 is the maximum number of time slots available for a port network.

Two TN2602AP circuit packs may be installed in a single port network (PN) for bearer duplication. In this configuration, one TN2602AP is an active IP media processor and one is a standby IP media processor. If the active media processor, or connections to the active media processor fail, active connections failover to the standby media processor and remain active. This duplication prevents active calls in progress from being dropped in case of failure. The interchange between duplicated circuit packs affects only the PN in which the circuit packs reside.

Note:

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. The call can be dropped, if these telephones are used while an interchange from active to standby media processor is in process.

Ensure that the Communication Manager license file has entries for each circuit pack and each entry has the identical voice channels enabled. Also ensure that both circuit packs include the latest firmware that supports bearer duplication.

Duplicated TN2602AP circuit packs and the Ethernet switch or switches that the circuit packs connect to must be in the same subnet. With this shared subnet, the Ethernet switches can use signals from the TN2602AP firmware to identify the MAC address of the active circuit pack. This identification process provides a consistent virtual interface for calls.

A single port network can have up to two TN2602AP circuit packs only. As result, the port network can have either two duplicated TN2602AP circuit packs or two load balancing TN2602AP circuit packs, but not both a duplicated pair and a load-balancing pair. However, in a Communication Manager configuration, some port networks can have a duplicated pair of TN2602AP circuit packs and other port networks can have a load-balancing pair of TN2602AP circuit packs. Some port networks can also have single or no TN2602AP circuit packs.

Note:

If a pair of TN2602AP circuit packs previously used for load balancing are re-administered to be used for bearer duplication, only the voice channels of whichever circuit pack is active can be used. For example, if you have two TN2602 AP circuit packs in a load balancing configuration, each with 320 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you have 320, not 484, channels available.

Installing the TN2602AP Media Resource 320

The following sections describe the installation process:

- [Checking your shipment](#) on page 35

- [Installing a TN2602AP IP Media Resource 320](#) on page 36
- [Installing the cables](#) on page 36
- [Installing the circuit packs](#) on page 37
- [Verifying installation and voice channels](#) on page 38
- [Administering the TN2602AP circuit pack](#) on page 38
- [Testing the external connection to the LAN](#) on page 40
- [Verifying active call status](#) on page 40
- [Upgrading firmware \(if necessary\)](#) on page 40

For further administration, see the *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Checking your shipment

When the order arrives at your site, check the contents. See [Table 4: Required Hardware](#) on page 35.

1. Inspect the shipping carton for damage before opening it. If the box is damaged, *do not open it*. Inform the shipping company, and ask for instructions on filing a claim.
2. If the box is undamaged, check the contents against the packing slip. Check the condition of each component, and note any damage or shortages on the packing slip. The carton should contain the items in [Table 4: Required Hardware](#) on page 35 for each TN2602AP IP Media Resource 320 circuit pack ordered.
3. Read and follow any directions inserted into the package by the factory.

Table 4: Required Hardware

Description	Quantity
TN2602AP IP Media Resource 320 (MedPro)	1 or 2/PN
Media Resource 320 Adapter ¹ with retainer clip	1/MedRes

¹The adapter has an amphenol connector on one side and an RJ45 connector and two Ethernet ports on the other side for connecting to the network. See [Media Resource 320 Adapter](#) on page 37.

Note:

You must provide one CAT5 or better cable for each TN2602AP.

Installing a TN2602AP IP Media Resource 320

Note:

Only two TN2602AP circuit packs are allowed per port network.

Have the following equipment and information on site before your shipment arrives:

Note:

If used in place of an Expansion Interface circuit pack in a mixed port network configuration, Avaya recommends that the TN2602AP circuit pack be installed in the A01 slot.

- One or two unoccupied port slots in the branch gateway for the TN2602AP circuit pack(s).
- One or two 10/100 BaseT Ethernet connections into your local area network (LAN)
- One or two valid, unused IP addresses on the network that can be assigned to the IP Media Resource 320 server. You also need the subnet mask, which should be the same for each of the TN2602AP circuit packs installed on the same port network. You may need the default gateway if the circuit pack handles off-subnet calls.

Note:

Get this information from the project manager or your network administrator.

Installing the cables

To install the cable for the IP Media Resource 320 circuit pack:

Note:

If used in place of an Expansion Interface circuit pack in a mixed port network configuration, Avaya recommends that the TN2602AP circuit pack be installed in the A01 slot.

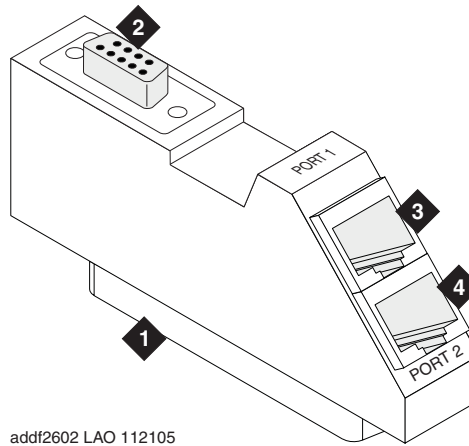
1. Determine into which port slots you are putting the TN2602AP circuit packs.

From the rear of the branch gateway:

Note:

To install the TN2602AP into an old carrier or cabinet, replace the WP cables that connect the backplane to the rear connector panel by Twisted Pair I/O cables to handle the 100-Mbps speed. For information on replacing the wires, see [Replacing the WP cables on page 40](#).

2. Connect the amphenol connector on the adapter to the Amphenol connector corresponding to each TN2602AP slot. See [Figure 4: Media Resource 320 Adapter](#).

Figure 4: Media Resource 320 Adapter**Figure notes:**

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. Amphenol connector to backplane connector corresponding to TN2602AP slot 2. RS-232 connector for services | <ol style="list-style-type: none"> 3. Port 1: RJ45 LAN cable connection for 100 Mbps CAT5 cable 4. Port 2: RJ45 LAN connection (not used) |
|---|---|

⚠ Important:

Plug the CAT5 cable into the top port labeled Port 1. Do not plug the CAT5 cable into the second port.

3. Connect the network cables to the Port 1 ETHERNET connector on the Media Resource 320 adapters on the backplane.
4. Snap the retainer clips over the adapters to hold them in place.

Installing the circuit packs**⚠ CAUTION:**

When adding or replacing any hardware, be sure to ground yourself against electrostatic discharge (ESD) by wearing a grounded wrist strap.

Note:

The TN2602AP circuit packs are hot-swappable, so you do not need to power down the branch gateway to install them.

Note:

To properly seat the circuit pack, push firmly on the front of the faceplate until the latch reaches the bottom rail of the carrier. Then close the latch until it is fully engaged.

To install the circuit pack:

- Insert the TN2602AP circuit pack into the port slot you reserved for the TN2602AP and seat the TN2602AP properly.

When you plug in the TN2602AP circuit pack, the system starts to boot. The RED LED stays on until the onboard firmware is operational.

Verifying installation and voice channels

To verify the installation:

1. Type `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP. Press **Enter**
2. Verify that the slot location displays TN2602AP.
3. Look in the Vintage column and note the firmware version. If the firmware version is earlier than the one on the Avaya Support Web site, you must upgrade the firmware on the circuit pack. See the Firmware Download Procedure document, which is posted on the Avaya Download Web site.
4. Type `display system-parameters customer-options` and press **Enter**.
5. Find the **Maximum TN2602 VoIP Channels:** field. Look at the Used column next to the field to see the maximum number of voice channels available.

Administering the TN2602AP circuit pack

To administer the circuit pack:

1. Type `change node-names ip` and press **Enter**.
2. Type the node names and IP addresses for the TN2602AP.
3. Type `display circuit-packs`. Verify that the TN2602AP shows up in the **Code** column. Press **Enter**.
4. Type `add ip-interface UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location. Press **Enter**.
5. Type the following information:
 - If administering two circuit packs as duplicated, in the **Critical Reliable Bearer?** field, type **y**.

Note:

If **Critical Reliable Bearer?** is yes, the system displays a second column of information. Fill in information for both circuit packs.

- The **Type**, **Slot**, **IP Address**, and **Code/Suffix** fields are populated automatically.
- In the **Node Name** field, type the same node name entered on the **Node Name** screen.

- In the **Subnet Mask** field, enter the subnet mask determined by the LAN administrator. This setting also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y**.
- In the **Gateway Address** field, use the address determined by the LAN administrator. This setting also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y**.
- Set the **Enable Ethernet Port** field to **y**.
- Set the **Net Region** field to **1** or another number determined by the LAN administrator. This setting also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y**.
- Set **VLAN** to **n**.
- Set the **VOIP Channel** field to **320**.
- Set the **Shared Virtual Address** field to the virtual IP address shared by the two TN2602AP circuit packs.
- Set the **Virtual MAC Table** field to a number from **1** to **4**. Normally, you can enter **1**. However, you might choose a different table number if all of the following conditions exist:
 - A port network under the control of a different Communication Manager main server has duplicated TN2602AP circuit packs.
 - That port network controlled by a different main server has the same number as the port network in which you are administering the TN2602AP circuit packs.
 - The port network or its main server connects to the same Ethernet switch as the port network in which you are administering the TN2602AP circuit packs.

To prevent two TN2602AP circuit packs within your network from having the same virtual MAC address, select a different Virtual MAC Table from that chosen for a port network that has the previously listed conditions.

- The **Virtual MAC Address** field is populated automatically with a MAC address from the Virtual MAC Table you select.
- Set Ethernet Options to match your network. Avaya recommends the following settings:
 - **Auto: y** (default)

If you enter **n**, also complete the following fields. The recommended values are displayed.

- **Speed: 100 Mbps**
- **Duplicated Server: Full**

6. Press **Enter** to save the information and effect the new settings.

Testing the external connection to the LAN

To test the external IP connections, ping a computer on the same subnet, the gateway, and a computer beyond the gateway. If everything is configured correctly, the `Result` column on the **Ping Results** screen reads **pass**. If it reads **abort**, verify the IP-address information and check the connectivity, including the cabling.

1. Type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of the TN2602AP IP Media Resource 320 and *UUCSS* is the cabinet, carrier, and slot location of a C-LAN circuit pack or another media processor circuit pack within the subnet. Press **Enter**.
2. If Step 1 passes, type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of an endpoint on your gateway and *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP circuit pack you are testing. Press **Enter**.
3. If Step 2 passes, type `ping ip-address ipaddress board UUCSS`, where *ipaddress* is the IP address of an endpoint beyond the gateway and *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP circuit pack you are testing. Press **Enter**.

Verifying active call status

To verify that calls are being processed:

1. Type `status media processor board UUCSS`, where *UUCSS* is the board location.
2. Look at the LINKS and DSP CHANNEL STATUS categories to determine whether calls are being processed.

Testing the circuit pack

Test the TN2602AP circuit pack with the command `test board UUCSS`. For more information, see the *Maintenance Commands for Avaya Aura® Communication Manager Branch Gateways and Servers*, 03-300431.

Upgrading firmware (if necessary)

If you determined that you must upgrade the firmware, do so now. For more information on firmware downloads and instructions for downloading, see <http://www.avaya.com/support/>.

Firmware upgrades

Firmware is upgraded the same way as the TN799DP C-LAN and TN2501AP VAL circuit packs. Resetting the circuit pack as part of the process affects the bearer traffic.

Replacing the I/O cables

Note:

You only need to replace the I/O cables for the TN2602AP circuit packs you are installing.

The existing I/O cables have straight, not twisted, wires. These cables can be mostly white with two red or multicolored. If the cables have multicolored, tightly twisted wires, no replacement is necessary.

**CAUTION:**

Turn off power to the carrier or the gateway before you replace the cables.

**CAUTION:**

When you add or replace any hardware and associated cables and adapters, ground yourself against electrostatic discharge (ESD). Always wear a grounded wrist strap.

To replace the existing I/O cables:

1. If the configuration includes a G600 Media Gateway, you must remove the fan assembly to access the cables. Loosen the thumb screws on the fan assembly and pull the fan straight out. See [G600 Media Gateway fan assembly removal](#) on page 42. Leave the fan assembly off until you install all the wires.
2. Note the orientation of the existing 10 cables. The existing I/O cables can be white and red or multicolored. These cables are not twisted.
3. Remove the I/O cables that you want to replace from the backplane and the connector panel slots.
4. Install the twisted pair I/O cables on the backplane to replace the cables you just removed. Use the correct orientation. See [Proper orientation for the twisted pair I/O cables](#) on page 43. Observe the white outline that is printed on the backplane for the location of each connector.
5. View the cables from the *wiring* side of the twin connectors. That is, view the cables while you plug the cables into the backplane. Connectors oriented correctly for plug-in look like the cables in [Proper orientation for the twisted pair I/O cables](#) on page 43.

The circled pin locations are *No-Connects*. At the top there is an orange-black pair on the right and a violet-brown pair on the left. Do not install wires in these locations.

If you are replacing I/O cables for all slot positions, plug all cables into the backplane before you match the *D* connector on each cable to the carrier frame.

You must install the 50-position metal shell *D* connectors into the carrier frame. Make sure

that the longer side of the *D* connector (pins 1 to 25) is toward the right when you view the pins from the rear of the branch gateway.

6. Apply the 10/100 mbps label to the front of the carrier slot. Apply the label over the slot label that corresponds to the slot where you installed the twisted pair I/O cable.
7. For the G600 Media Gateway, replace the fan unit if you are not adding any branch gateways. If you are adding more branch gateways to the rack, leave the fan units off until you install all the TDM cables.

Figure 5: G600 Media Gateway fan assembly removal

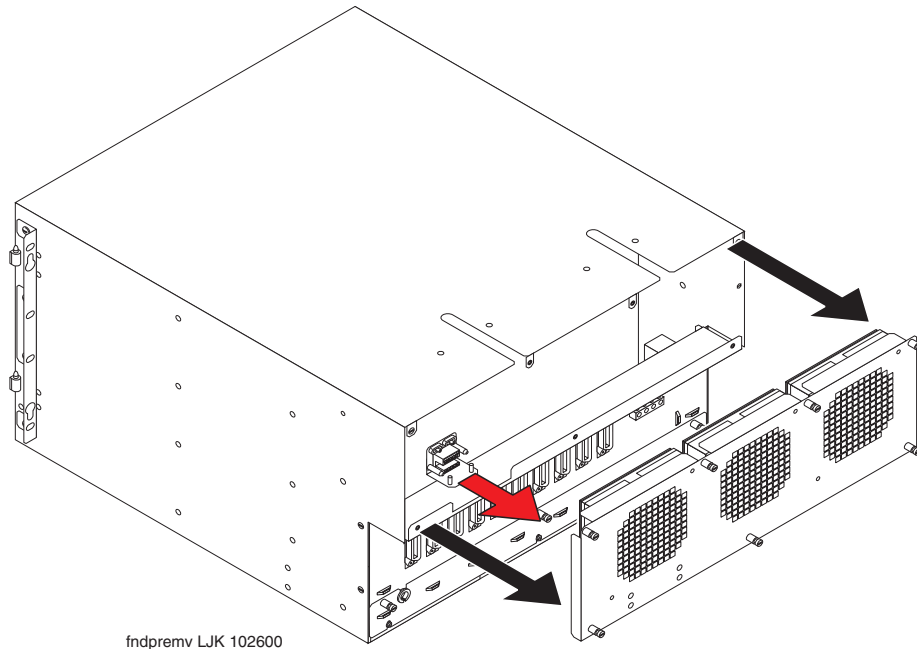


Figure 6: Proper orientation for the twisted pair I/O cables

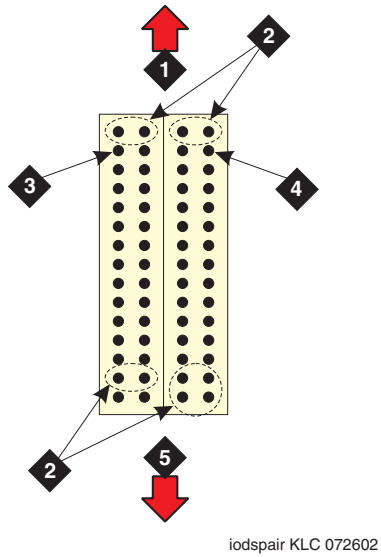


Figure notes:

- | | |
|--------------------------|-----------------|
| 1. Top | 4. Orange-black |
| 2. No connects, no wires | 5. Bottom |
| 3. Violet-brown | |
-

Chapter 3: Trunks and lines

This chapter provides procedures for adding analog and digital trunks and lines to an existing branch gateway. These procedures are examples only. Actual wiring procedures might vary at each site.

List of analog and digital trunk and line circuit packs

[Table 5: Analog and digital trunk and line circuit packs](#) lists the circuit packs currently sold sorted by apparatus code, including those used in non-United States installations.

Table 5: Analog and digital trunk and line circuit packs

Apparatus Code	Name
TN2147C	Central Office Trunk—multiple countries, 8 ports
TN2181	DCP Digital Line, 2-Wire, 16 ports
TN2183	Analog Line—multiple countries, 16 ports
TN2198BP	ISDN-BRI 2-Wire U Interface, 12 ports
TN2199	Central Office Trunk—Russia, 3-wire, 4 ports
TN2224CP	DCP Digital Line, 2-Wire, 24 ports, Firmware Download Enabled
TN2313AP	DS1 Interface Trunk, 24 channels; Firmware Download Enabled
TN429D	Direct Inward/Outward Dialing (DIOD) or CO Trunk, 8 ports
TN436B	Direct Inward Dialing (DID) Trunk—Australia, 8 ports
TN464HP/ TN2464CP	DS1 Interface Trunk—T1, 24 Channel; E1, 32 Channel; Firmware Download Enabled
TN465C	Analog Central Office Trunk—Multi-country, 8 ports
TN556D	ISDN-BRI, S/T-NT Interface, 4-Wire, 12 ports
TN747B	Central Office Trunk, 8 ports
TN753B	Direct Inward Dialing (DID) Trunk, 8 ports
1 of 2	

Table 5: Analog and digital trunk and line circuit packs (continued)

Apparatus Code	Name
TN754C	DCP Digital Line, 4-Wire, 8 ports
TN760E	Tie Trunk, 4-Wire, 4 ports
TN763D	Auxiliary Trunk, 4 ports
TN767E	DS1 Interface Trunk—T1, 24 Channel
TN793CP	Analog Line with Caller ID, 24 ports
TN797	Analog CO Trunk or Line Combo—US, Canada, 8 ports
2 of 2	

For more information on installing analog and digital trunk and line circuit packs, see:

- [Adding TN464HP/TN2464CP with echo cancellation](#) on page 46
- [Adding CO, FX, WATS, and PCOL](#) on page 48
- [Adding DID trunks](#) on page 49
- [Adding Analog Tie trunks](#) on page 49
- [Adding digital DS1 Tie trunks and OPS](#) on page 51
- [Adding TTC Japan 2-Mbit trunk](#) on page 51
- [Adding CAMA/E911 trunk](#) on page 52
- [Adding ISDN—PRI](#) on page 56

Adding TN464HP/TN2464CP with echo cancellation

The TN464HP and TN2464CP circuit packs with echo cancellation are intended for customers who are likely to encounter echo over circuits connected to the Direct Distance Dialing (DDD) network. These circuit packs are intended for channels supporting voice. Therefore, the TN464HP and TN2464CP circuit packs support the following trunks: CAS, CO, DID, DIOD, DMI, FX, Tie, and WATS. The TN464HP and TN2464CP circuit packs do not support any data trunk groups.

Note:

The P suffix designation means the circuit pack is programmable. New firmware can be downloaded to the circuit pack.

The TN464HP and TN2464CP circuit packs are backwards compatible. However, you can use the echo cancellation feature only with Release 1.1 or later of Communication Manager and after the feature is enabled.

The echo cancellation feature cancels echoes with delays up to 96 milliseconds. The system disables echo cancellation automatically when the circuit pack detects a 2100-hertz *phase-reversed* tone replaced by high-speed modems (56 kilobaud). Echo cancellation does not disable when the circuit pack detects a 2100-hertz *straight* tone generated by low-speed modems (9.6 kilobaud).

For more information about installing port circuit packs, see [Installing the circuit pack](#) on page 53. For more information about setting the option switches, see the job aid titled *Option Switch Settings*, 555-245-774. For more information about circuit pack administration, see *Administering Avaya Aura® Communication Manager*, 03-300509.

You must first purchase the echo cancellation and then activate the echo cancellation by the license file. See *Administering Avaya Aura® Communication Manager*, 03-300509.

Use the following procedure to modify the settings:

Note:

You do not need to busyout the circuit packs to modify the settings. But the modified settings do not take effect until you busy out the port or run the scheduled maintenance.

1. Type **display system-parameters customer-options** and press **Enter**. Verify that the **DS1 Echo Cancellation?** field is set to **y**. If not, contact your Avaya representative because the license file determines this setting.
2. Type **add ds1 *UUUSS***, where *UUUSS* is the cabinet, carrier, and slot location, and press **Enter**.
3. On the **DS1 Circuit Pack** screen, set the **Echo Cancellation?** field to **y**.
When set to **y**, the system displays two new fields: **EC Direction:** and **EC Configuration:**.
 - If you know the echo is coming into the system, keep the default setting for the **EC Direction:** field of **inward**.
 - If the distant party is hearing echo that originates in either the system, the line side stations, or system equipment, set the **EC Direction:** field to **outward**.
 - Keep the default setting for the **EC Configuration:** field.
4. Type **add trunk-group next** and press **Enter**.
5. On **Trunk Features**, set the **DS1 Echo Cancellation?** field to **y**.
6. Test the voice quality on a telephone connected through the TN464HP or TN2464CP circuit packs and known to have echo to determine if the echo was eliminated.
7. If the echo still exists, reset the **EC Configuration:** field and test the voice quality. These settings provide help for the following scenarios:

- Setting 1 rapidly minimizes echo when first detected, regardless of how loud the speaker is. Settings 1 and 4 have the same EC settings except that Setting 1 introduces 6 dB of loss.
 - Setting 2 minimizes speech clipping, but the echo takes a fraction of a second longer to fade.
 - Setting 3 eliminates speech clipping, but a strong echo might take 2 or 3 seconds to fade.
 - Setting 4 minimizes strong echo, hot signals, or excessive clipping or breakup of speech from a distant party. Setting 4 reduces speech clipping but slight residual echo or more background noise might remain.
8. If the echo still exists after you try all these settings, contact technical support.

Adding CO, FX, WATS, and PCOL

Each of the following trunks connects to one port of an 8-port TN747B Central Office trunk or to one of an assortment of North American Central Office trunk circuit packs:

- Central Office (**CO**) trunk
- Foreign Exchange (**FX**) trunk
- Personal Central Office Line (**PCOL**)
- Wide Area Telecommunications Service (**WATS**) trunk

Before physically installing the circuit pack, you need the assigned slot location (UUCSS). UU is the gateway or port network number (G650). C is the media gateway (G650) or carrier. SS is the slot location. This information is available from the person who administered the translations, most likely the software specialist. If the information is not available, you can find the information on the **Trunk Group Status** screen.

1. Get the trunk group number from the administrator.
2. Type **status trunk-group number** and press **Enter**.
3. Install the CO trunk circuit pack in the assigned carrier slot.

Use the correct type of trunk circuit pack with enough ports to handle the number of trunks you need. For more information on finding out the number of circuit packs you need, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

4. Administer the screens listed in "Adding a **CO**, **FX**, or **WATS** Trunk Group" and "Adding a PCOL Trunk Group" in *Administering Avaya Aura® Communication Manager*, 03-300509.

Adding DID trunks

Each Direct Inward Dial (**DID**) trunk connects to one of the following:

- one port of a DID Trunk circuit pack
- one port of an assortment of global **DID/DIOD** trunk circuit packs.

Before physically installing the circuit pack, you need the assigned slot location (UUCSS). UU is the media gateway or port network number (G650). C is the media gateway (G650) or carrier. SS is the slot location. The information is available from the person who administered the translations, most likely the software specialist. If the information is not available, you can find the information on the **Trunk Group Status** screen.

1. Get the trunk group number from the administrator.
2. Type **status trunk-group number** and press **Enter**.
3. Install a **DID/DIOD** trunk circuit pack in the assigned carrier slot.
4. Administer the screens listed under Adding a **DID** Trunk Group in *Administering Avaya Aura® Communication Manager* (03-300509).

Adding Analog Tie trunks

Each analog tie trunk connects to one port of a 4-port tie trunk circuit pack or to an assortment of global tie trunk circuit packs.

Before physically installing the circuit pack, you need the assigned slot location (UUCSS). UU is the gateway or port network number (G650). C is the media gateway (G650) or carrier. SS is the slot location. The information is available from the person who administered the translations, most likely the software specialist. If this information is not available, you can find the information on the **Trunk Group Status** screen.

1. Get the trunk group number from the administrator.
2. Type **status trunk-group number** and press **Enter**.
3. Install the analog or global tie trunk circuit pack in the assigned slot.
4. Obtain information on setting the option switches and administering the port for customer-owned tie-trunk facilities. An example of a customer-owned, not leased, tie-trunk facilities is a campus environment. With customer-owned tie-trunks, the TN760E tie trunk circuit pack provides signaling capabilities beyond those specified by the industry-wide **E&M** standard.

For more information about setting the option switches and administering the port, see [Figure 7: TN760E Tie Trunk circuit pack option switches \(component side\)](#) on page 50 and

[Table 6: TN760E Analog Tie Trunk circuit pack option switch settings and administration](#) on page 50.

5. Administer the screens listed under Adding a Tie Trunk Group in *Administering Avaya Aura® Communication Manager* (03-300509).

Figure 7: TN760E Tie Trunk circuit pack option switches (component side)

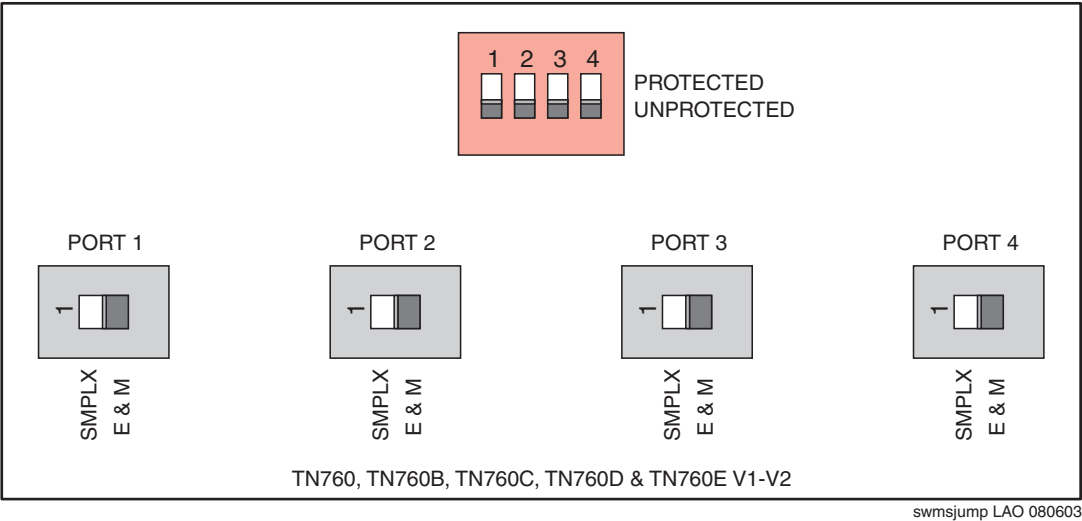


Table 6: TN760E Analog Tie Trunk circuit pack option switch settings and administration

Installation situation		Preferred signaling format		E&M/ SMPLX option switch	Set Prot/ Unprot option switch	Administered port*
Circumstance	To	System	Far-End			
Collocated	Media Gateway	E&M Type 1 Compatible	E&M Type 1 Standard	E&M	Unprotected	Type 1 Compatible
Inter-Building	Media Gateway	Protected Type 1 Compatible	Protected Type 1 Standard Plus Protection Unit	E&M	Protected	Type 1 Compatible
Collocated	Net Integrated	E&M Type 1 Standard	Any system	E&M	Unprotected	Type 1

*. Administer the items in this column on the **Trunk Group** screen.

Adding digital DS1 Tie trunks and OPS

The following circuit packs provide connections to a 1.544-Mbps **DS1** facility (T1) as 24 independent 64-kbps trunks and a 2.048-Mbps **DS1** facility (E1) as 32 independent 64-kbps trunks:

- TN2313 DS1 Tie Trunk
- TN767B (or later) DS1 Interface
- TN464HP (or later) DS1 Interface

Note:

Because adding **DS1** tie-trunk service might require a service interruption, notify the customer in advance as to when you will be adding the circuit pack(s).

For more information about administering DS1 Tie Trunks, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Adding TTC Japan 2-Mbit trunk

The TN2242 Japan 2-Mbit trunk connects the media gateway to other vendor equipment in Japan and to other MultiVantage configurations through the Time Division Multiplexor (TDM).

Before physically installing the circuit pack, you need the assigned slot location (UUCSS). UU is the media gateway or port network number (G650). C is the media gateway (G650) or carrier. SS is the slot location. The information is available from the person who administered the translations, most likely the software specialist. If the information is not available, you can find the information on the **Trunk Group Status** screen.

1. Get the trunk group number from the administrator.
2. Type **status trunk-group number** and press **Enter**.
3. Install a TN2242 trunk circuit pack in the assigned slot.
4. Connect the H600-513 cable from the media gateway to the Time Division Multiplexor device.
5. To administer screens, see *Administering Avaya Aura® Communication Manager*, 03-300509:
 - For ISDN applications, see ISDN Service.
 - For non-ISDN applications, see Managing Trunks.

Adding CAMA/E911 trunk

The Centralized Automatic Message Accounting (CAMA)/E911 feature requires the TN429C/D (or later) CO Trunk circuit pack.

Port networks in which TN429C/D circuit packs connect to CAMA trunks require some Call Progress Tone Receiver (CPTR) resources to be either TN744D V2 or TN2182B circuit packs. These resources are required because Touch Tone Receiver (TTR)/CPTR or General Purpose Tone Receiver (GPTR) resources are selected from the available pool in the port network when needed.

[Table 7: Compatibility Tone Clock, TTR/CPTR, and GPTR circuit packs](#) on page 52 denotes which of these circuit packs are compatible and which are not affected.

Perform the following tasks to add CAMA/E911 trunks:

- [Installing the circuit pack](#) on page 53
- [Adding the trunks](#) on page 53
- [Changing the feature access code](#) on page 54
- [Changing the ARS digit analysis](#) on page 54
- [Changing the route patterns](#) on page 55
- [Changing the CAMA numbering and class of restriction](#) on page 55

Table 7: Compatibility Tone Clock, TTR/CPTR, and GPTR circuit packs

Circuit Pack	Description	Compatibility with CAMA Trunks in Same PN	Application	Notes
TN744D,V2 TN744E,V1	Call Classifier - Detector	Not Compatible	Used globally	8 GPTR/call classification ports. Use TN744D, V2 or later to support the CAMA feature.
TN744D,V2 TN744E,V1	Call Classifier - Detector	Compatible	Used globally	8 GPTR/call classification ports. Required in PN supporting CAMA trunks if GPTR resources are required in excess of those on the TN2182BV2 (or later). Also required, if the TN768 or TN780 tone clocks are used, in place of TN748.
				1 of 2

Table 7: Compatibility Tone Clock, TTR/CPTR, and GPTR circuit packs (continued)

Circuit Pack	Description	Compatibility with CAMA Trunks in Same PN	Application	Notes
TN748C/D	Touchtone Detector / Call Progress Tone Detector	Not Compatible	Used in the U.S. and a few other countries	4 TTR and 2 CPTR ports. Use TN744D, V2 or later to support the CAMA feature.
TN780	Tone Clock	Not Affected	Used in the U.S. (infrequently) for Stratum 3 clocking and used in many other countries	Tone clock only, no TTR/CPTR functionality. Usually found with TN748 circuit packs in the U.S. Use TN744D, V2 or later to support the CAMA feature.
TN2182B/C	Tone Detector/ Tone Generator/ Call Classifier	Compatible	Used globally	Tone clock plus 8 GPTR/call classification ports. Use TN2182B to support the CAMA feature.
				2 of 2

Installing the circuit pack

The install the circuit pack:

1. Insert the TN429C or later CO Trunk circuit pack in any available port slot. Ensure that the TN744D Call Classifier/Detector circuit pack is Vintage 2 or later or use the TN744E.
2. Connect the CAMA trunk to the Main Distribution Field, the trunk from the CO. For more information, see the Circuit Pack and Auxiliary Equipment Leads (Pinout Charts) in the job aid titled *Connector and Cable Diagrams (Pinout Charts)* (555-245-773).

Adding the trunks

The add trunks to a group:

Note:

So that this trunk group does not get buried within the other trunk groups, use a distinctive trunk group number such as 99.

1. Type **add trunk 99** and press **Enter**.

Trunks and lines

2. In the **Group Type** field, type `cama`.
3. In the **Group Name** field, type the desired name.
4. In the **TAC** field, type the desired trunk access code.
5. In the **Outgoing Display** field, type `y`.
6. In the **CESID I Digits Sent** field, type the number directed by the Central Office (CO) or the Public Safety Answering Point (PSAP).
7. Go to the **Administrable Timers** screen. Adjust these fields according to your CO.
8. Go to the **Group Member Assignments** screen.
9. In the **Port** field, add the trunk members.
10. Press **F3** when finished to submit the form and effect the changes.

Changing the feature access code

To change the feature access code:

1. Type `change feature-access-code` and press **Enter**.
2. In the **Auto Route Selection (ARS) Access Code 1:** field, administer the ARS access code and press **Enter**. In the example above, the ARS access code is **9**. The ARS access code must match the dial plan.

Changing the ARS digit analysis

To change the ARS digit analysis:

1. Type `change ars analysis number` and press **Enter**. The example uses the number 9.
2. In the **Dialed String** field, in the first empty row, type 11.
3. In the **Total Mn** field, type 2.
4. In the **Total Mx** field, type 2.
5. In the **Rte Pat** field, type the desired Route Pattern. In the example, the route pattern is 11.

Note:

For the following step, if you are using the Attendant Crisis Alerting feature, type `alrt` instead of `emer`.

6. In the **Call Type** field, type `emer`.
7. On the next empty row, in the **Dialed String** field, type 911.
8. In the **Total Mn** field, type 3.

9. In the **Total Mx** field, type 3.
10. In the **Rte Pat** field, type the desired Route Pattern. In the example, the route pattern is 12.

Note:

For the following step, if you are using the Attendant Crisis Alerting feature, type **alrt** instead of **emer**.

11. In the **Call Type** field, type **emer** and press **Enter**.
12. Press **F3** to submit the screen and effect the changes.

Changing the route patterns

To change the route patterns:

1. Type **change route-pattern number**, the route pattern to be changed, and press **Enter**. In the example, the route pattern is 11.
2. In the **Grp. No.** field, type the CAMA trunk group number.
3. In the **FRL** field, type 0.

Note:

For the following step, if the service provider Central Office (CO) wants KP11ST as the dialed digit string, leave the **Inserted Digits** field blank. If the CO wants KP911ST, type 9 in the **Inserted Digits** field.

4. Administer the **Inserted Digits** field if needed and press **Enter**.
5. Type **change route-pattern number**, the route pattern to be changed, and press **Enter**. In the example, the route pattern is 12.
6. In **Grp. No.** field, type the CAMA trunk group number.
7. In the **FRL** field, type 0.

Note:

For the following step, if the service provider Central Office (CO) wants KP911ST as the dialed digit string, leave blank. If the CO wants KP11ST, delete one digit.

8. Administer the **No. Del Digits** field, if needed.
9. Press **F3** to submit the screen and effect the changes.

Changing the CAMA numbering and class of restriction

To change the CAMA numbering and class of restriction:

1. Type **change cama-numbering** and press **Enter**.

2. In the **System CESID Default** field, type your own system default.

This system default is the number that the 911 operator sees when the extension code is not found in the CAMA Numbering table.

3. In the **Ext Len**, **Ext Code**, **CESID**, and **Total Length** fields, fill out your own CAMA numbering plan. Be sure to cover all extensions.
4. Press **F3** to submit the screen and effect the changes.
5. Type **change cor number**, which is the class of restriction (COR) to be changed, and press **Enter**.
6. Change all CORs that are defined for stations to remove any calling party restrictions for 911 calls.
7. In the **Calling Party Restriction:** field, type **none**.
8. Press **F3** to submit the screen and effect the changes.
9. Type **save translations** and press **Enter**. This command takes all translation information in memory and writes it to the hard disk drive.

Adding ISDN—PRI

North American

To add ISDN-PRI:

1. Install a TN767E (or later) DS1 or a TN464HP DS1/E1 circuit pack for a signaling link and up to 23 **ISDN—PRI** Trunk Group members.
2. If the port network does not have a TN2312AP IPSI circuit pack, install a TN2182 Tone-Clock circuit pack. The Tone-Clock circuit pack provides synchronization for the **DS1** circuit pack.

International

The following steps add ISDN-PRI.

1. Install a TN464HP DS1/E1 circuit pack for the assignment of the 2 signaling channels and up to 30 **ISDN — PRI** Trunk Group members. Each E1 span provides 32 ports.
2. If the port network does not have a TN2312AP IPSI circuit pack, install a TN2182 Tone-Clock circuit pack. The Tone-Clock circuit pack provides synchronization for the DS1/E1 circuit pack.

Adding circuit packs

Before physically installing the circuit pack, you need the assigned slot location (UUCSS). UU is the gateway or port network number. C is the gateway or carrier. SS is the slot location. To obtain this information, contact the person who administered the translations, for example, the software specialist, or see the **Trunk Group Status** screen.

1. Get the trunk group number from the administrator.
2. Type **status trunk-group number** and press **Enter**.
3. Install the DS1 Interface circuit pack in the assigned slot.
4. Install a Tone Detector circuit pack, if required.

Connecting cables

To connect the cables to the MDF.

- Install and connect cables from the TN464HP to the Main Distribution Field as required.

Administering the circuit pack

To administer the circuit pack:

- Administer the screens listed under ISDN Trunk Group and Trunk Group screens in *Administering Avaya Aura® Communication Manager* (03-300509). These screens are described in the Screen Reference chapter.

Resolving alarms

To display the alarms:

1. Type **display alarms** and press **Enter**.
2. Examine the alarm log. Resolve any alarms that might exist using the appropriate maintenance document.

Saving translations

To save translations:

1. Type **save translation** and press **Enter**. With this command, the system writes all translation in the system memory to the hard disk drive.

Chapter 4: Port networks

This chapter contains information and procedures for adding a port network to an existing system. The new port network consists of one to five TDM-cabled G650 Media Gateways.

To add a port network, complete the following tasks:

- [Installing a G650 Media Gateway](#) on page 59
- [Installing the IPSI circuit pack](#) on page 59
- [Assigning IP addresses to the IPSI circuit packs](#) on page 60
- [Administering the port network](#) on page 63
- [Installing additional circuit packs](#) on page 65

The servers can support configurations that contains:

- single control networks
- duplicated control networks
- single IP-PNC bearer networks
- IP-PNC networks with duplicated control and duplicated bearer

Installing a G650 Media Gateway

For more information about physically installing the G650 Media Gateways and connecting the gateways to the MDF or patch panels, see *Installing the Avaya G650 Media Gateway*, 03-300685.

Installing the IPSI circuit pack

Once you have installed all the branch gateways, install the TN2312BP IP Server Interface (IPSI) circuit pack in the branch gateway. Install this circuit pack in the A position, slot A01.

Duplicated server: If you have a duplicated control network, then install a second IPSI in the branch gateway in the B position, slot B01.

1. Install the IPSI adapter to the connector associated with slot 1 on the backplane.
2. Insert the TN2312BP IP Server Interface circuit pack into slot 1.

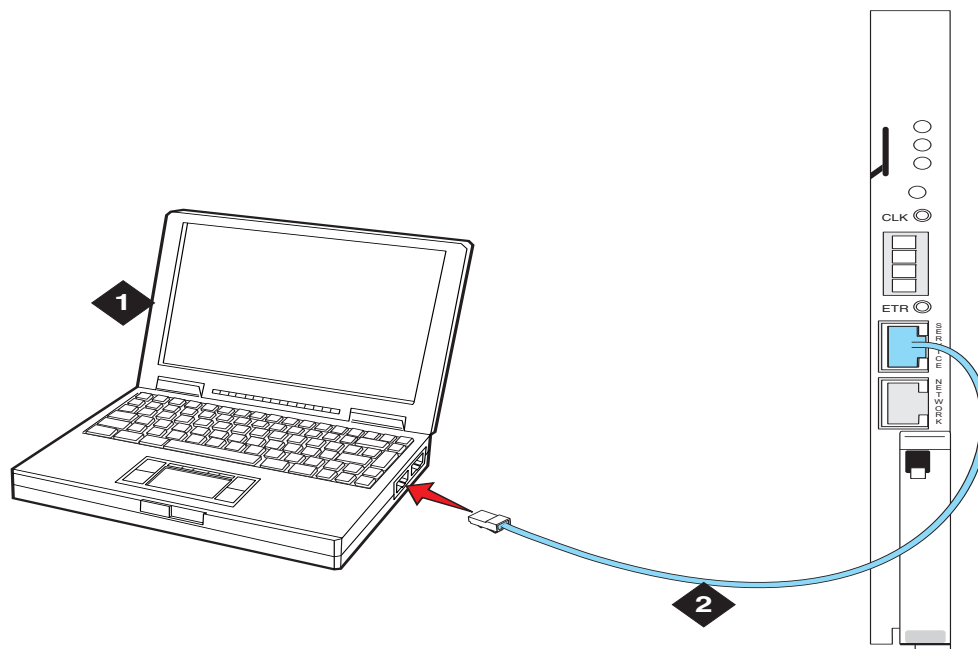
3. Connect a CAT5 cable to the RJ45 connector on the IPSI adapter.
4. If not already connected, connect the other end of the CAT5 cable to the next available port on the Ethernet switch.
5. If you are using one, connect one end of the serial maintenance cable to the 9-pin serial port connector on the IPSI adapter.

Assigning IP addresses to the IPSI circuit packs

Once the IPSI is installed, you must assign a static IP address.

You can administer static IP addresses for the IPSI circuit packs directly through the Ethernet port connection on the IPSI faceplate switch, which is the top port. See [Figure 8: Connecting directly to the IPSI](#).

Figure 8: Connecting directly to the IPSI



cadlipsi LAO 120711

Figure notes:

1. Services laptop
2. CAT5 cross-over cable to IPSI

Note:

Ensure that you have the password before you continue.

Clearing the ARP cache on the laptop

If you enter a new IP address and your computer cannot connect, clear the Address Resolution Protocol (ARP) cache.

To clear the ARP cache on the laptop:

1. Click **Start > Run**.
2. In the Run dialog box, type **command** and press **Enter**.
3. In the MS-DOS command line window, type **arp -d 192.11.13.6** and press **Enter**.

You obtain one of the following responses:

- A command line prompt to indicate that the cache is cleared.
 - **The specified entry was not found** message to indicate that the specified IP address does not currently display in the ARP cache.
4. To again access to the server, type **ping -t 192.11.13.6**, where **-t** is for the ping to repeat until the system generates a response. You get a response in about 3 minutes. Wait an additional 30 seconds before going back to the Web interface.
 5. To stop the ping, type **ctrl c**.
 6. Close the MS-DOS window.

Logging in to the IPSI

To log in to the IPSI:

1. Connect to the IPSI using SSH with the IP address **192.11.13.6**.

Prompt = [IPSI]:

Note:

Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **help** or **?**.

2. Type **ipsilogin** and press **Enter**. The abbreviated command is **il**.

Note:

The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log back in as **craft**.

Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type `show control interface` and press **Enter**.
2. To see the current settings, type `show port 1` and press **Enter**.
3. Type `set control interface ipaddr netmask`, where *ipaddr* is the customer-provided IP address and *netmask* is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN

[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: █
```

4. To save the changes and exit the IPSI session, type `quit` and press **Enter**.
5. Log in using SSH with the address **192.11.13.6**.
6. Type `show control interface` and press **Enter**.
The system displays the IP address, the subnetmask, and the default gateway information.
7. Verify that the correct information was entered.
8. If a default gateway is used, enter the gateway IP address.
Type `set control gateway gatewayaddr`, where *gatewayaddr* is the customer-provided IP address for their gateway and press **Enter**.
9. To save the changes and exit the IPSI session, type `quit` and press **Enter**.
10. Log in using SSH with the address **192.11.13.6**.
11. To verify the administration, type `show control interface` and press **Enter**.
12. To see the changes, type `exit` and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **craft**.
2. To display the quality of service values, type **show qos** and press **Enter**.
3. You can use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

Note:

Use **Help** to obtain syntax guidelines for these commands.

- Type **set vlan priority 6**
 - Type **set diffserv 46**
 - Type **set vlan tag on**
 - Type **set port negotiation 1 disable**
 - Type **set port duplex 1 full**
 - Type **set port speed 1 100**
4. To check the administered values, type **show qos** and press **Enter**.
 5. To exit, type **quit** and press **Enter**.



Important:

Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **set port** commands in step 3.

Administering the port network

Once the port network is installed, you must add translation information to the server. Use Secure Shell to access SAT commands.

Note:

For port networks using G650 Media Gateways, a cabinet is defined as up to 5 G650 Media Gateways mounted in a rack and TDM-connected.

1. Type **add cabinet number** where **number** is the next available number, up to 64, and press **Enter**.
2. Fill in the location and carrier type for media gateways 2, 3, 4, and 5.
3. Repeat Step 1 through Step 3 for each G650 media gateway stack controlled by one TN2312BP IPSI circuit pack.

Adding IPSI translations to Communication Manager

To add IPSI translations to Communication Manager:

1. Type `add ipserver-interface PN`, where *PN* is the port network 1-64 and press **Enter** to add the IPSI circuit pack information.
2. In the **Host:** field, type the IP address for the IPSI. This IPSI is located in the port network and is listed in the **Location:** field.
3. Set the **IP Control?** field to **y**.
4. Verify that all the other fields are populated.
5. Press **Enter** to effect the changes.
6. Repeat Steps 1 through 6 for each port network.

Setting IPSI duplication for duplicated control network only

To add a duplicated control PN to an existing port network system, where the port network is IP-PNC:

Use the following steps to enable IPSI duplication in a duplicated control network.

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

The system displays the following screen when the **IP-PNC?** field on the **Customer Options** screen is set to **y**. In this case, all port networks in the system are IP-PNC only.

```

change system-parameters duplication                               Page 1 of 1
                        DUPLICATION RELATED SYSTEM PARAMETERS

                        Enable Operation of IPSI Duplication? y
  
```

2. Set the **Enable Operation of IPSI Duplication?** field to **y**.
3. Press **Enter** to effect the changes.

Setting alarm activation level

To set the alarm activation level;

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

2. In the **CPE Alarm Activation Level** field, select **none** (default), **warning**, **minor**, or **major**, depending on the level you want.

Verifying IPSI translations

To verify that Communication Manager identifies the:

1. Type `list ipserver-interface` and press **Enter**.
2. Verify that the ISPI circuit pack is translated.

Verifying IPSI connectivity

To verify that the IPSI is connected to the network:

1. Under Diagnostics, click **Ping**.
2. Select **IPSI with cab number (1–99) ____ carrier number ____**. Fill in the blanks with the correct cabinet and carrier numbers.
3. Click **Execute Ping**.
4. Verify that the endpoints respond correctly.

Installing additional circuit packs

If you are adding circuit packs, install them now. For more information about installing and administering various circuit packs, see [Chapter 2: IP connectivity hardware](#) on page 19.

Chapter 5: Adjuncts and peripherals

This chapter provides procedures for installing software adjuncts and equipment peripherals to Avaya servers and gateways. Not all adjuncts and peripherals are addressed here.

Avaya servers and gateways can work with a wide range of external equipment, applications, and peripherals. For the purpose of this chapter:

- Adjuncts are software products that work with the various Avaya servers or branch gateways.
- Peripherals are hardware products that connect directly or remotely to Avaya servers or branch gateways.

Be aware that some equipment and software work only with certain releases. See your Avaya representative for the most current compatibility information.

Terminal server installation

This section provides information about connecting adjunct equipment to the C-LAN circuit pack or Internet connection on the S8300D Server using a terminal server. See [Figure 9: Switch-to-adjunct LAN connectivity through a terminal server](#) on page 68. Avaya supports the IOLAN+ 104 terminal server, which is RoHS compliant.

Any device that does not support a direct TCP/IP connection but does support an RS232 interface can connect through a terminal server. System printers, property management systems (PMS), and some CDR devices use RS232 connections and can connect through a terminal server.

You can connect up to four adjuncts through one terminal server.

Figure 9: Switch-to-adjunct LAN connectivity through a terminal server

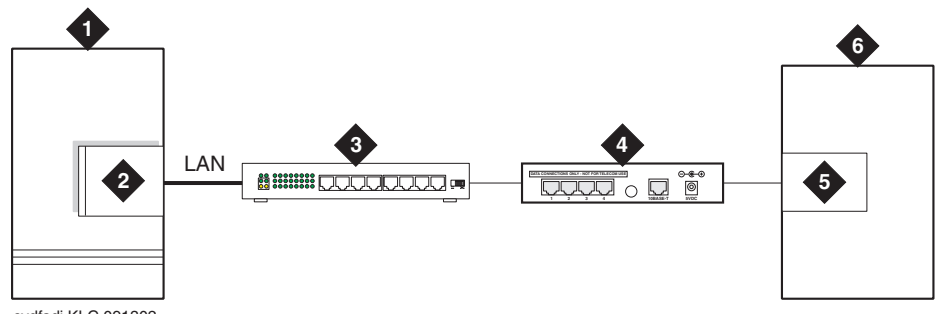


Figure notes:

- | | |
|--|--------------------|
| 1. Switch | 4. Terminal server |
| 2. C-LAN circuit pack or IP connection on an S8300D/G700 or G350 | 5. Serial port |
| 3. 10/100Base-T Hub (optional) | 6. CDR adjunct |

Installing and administering the terminal server

Ensure that you have the following equipment on site before the installation:

Table 8: Required equipment

Description	Qty	Supplier
IOLAN+ 104 communications server	1	Avaya
RJ45-to-DB25 connector for IOLAN+ (supplied with 700015084)	4	Avaya
DB25-to-DB9 connector for PC COM port	1	Avaya
RS232 Null modem (if needed for PC or printer connectivity)	1 or more	Avaya
Male/female adapter (if necessary)	1 or more	Avaya
6-inch RJ45 crossover cord, or	1	Avaya
10/100Base-T auto-sensing LAN hub or router	1	Customer
259A adapter, or	1	Avaya
CAT5 cross connect hardware and connecting blocks		Customer
RJ45 UTP Category 5 modular cords	1–2	Customer
451A in-line RJ45 adapters, as needed to connect modular cords together		

You also need a computer (laptop) with the HyperTerminal software program for the initial administration of the IOLAN+ and to set up the ports.

The general process is to

- Connect the IOLAN+ to the adjunct and the LAN.
- Administer the ports on the IOLAN+ with a PC or laptop at the local site.
- Test the connectivity back through the switch.

Distance limits

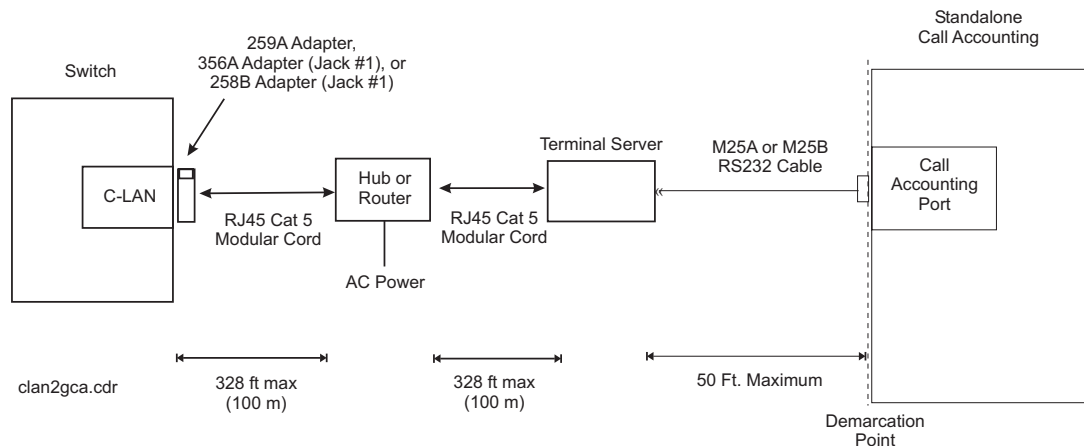
The distance limit from the switch to the LAN hub is 328 feet (100 meters). The distance limit from the LAN hub to the terminal server is 328 feet (100 meters). If installed, the limit from the terminal server to the adjunct is 50 feet (15 meters).

However, to achieve greater distance limits, the LAN hub/router of the switch might be connected to a WAN. In addition, the hub/router for the terminal server might also connect to the same WAN.

Cable connection diagram

[Figure 10: Stand-alone call accounting system link with a terminal server](#) shows the connection between the terminal server port and a call accounting system.

Figure 10: Stand-alone call accounting system link with a terminal server



Note:

You can connect the C-LAN circuit pack or S8300D Server directly to the terminal server with a data crossover cable. This connection eliminates the need for a hub or router in the middle. This connection also allows the C-LAN circuit pack or S8300D Server and the terminal server to communicate only with each other. With this connection, the C-LAN circuit pack or S8300D Server and the terminal server must be configured with the same subnet.

Making the connections

Connect the adjunct to the IOLAN+, using the RJ45-to-DB25 cable and the null modem. You can use a male/female adapter. See [Figure 11: Connecting an adjunct to the IOLAN+](#).

Figure 11: Connecting an adjunct to the IOLAN+

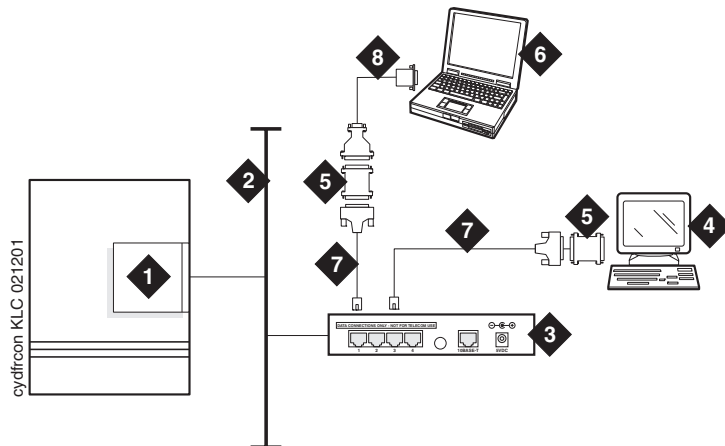


Figure notes:

- | | |
|--|--|
| 1. C-LAN circuit pack or IP connection on an S8300D/G700 or G350 | 5. Null modem |
| 2. Local area network (LAN) | 6. PC or laptop for initial administration |
| 3. IOLAN+ 104 terminal server | 7. DB25-to-RJ45 cable |
| 4. Adjunct, for example system management terminal or a system printer | 8. DB25-to-DB9 cable |

Follow these typical steps:

Note:

Depending on the connections for the adjunct, you might not need all these pieces.

1. Connect the null modem adapter to COM1 port on the adjunct.

Note:

The null modem is an important element in this setup. Without the null modem, data might not transfer correctly.

2. Connect the other end of the null modem adapter to the DB25-to-RJ45 cable.
3. Connect the RJ45 end to any port on the IOLAN+.

Administering the IOLAN+

To administer the IOLAN+ the first time, you must connect a PC or laptop to the RS232 Port 1 on the IOLAN+ terminal server. Follow these typical steps:

Note:

Depending on the COM port of the computer, you might not need all these pieces.

1. Connect the DB9 end of the DB9-to-DB25 cable to the COM port on the PC or laptop.
2. Connect the DB25 end to the null modem adapter.
3. Connect the other end of the null modem adapter to the DB25 to RJ45 cable.
4. Connect the RJ45 end to Port 1 of the IOLAN+.

Before starting the initial administration, ensure that you have the following information:

- New IP address and subnet mask for IOLAN+
- Host name for IOLAN+
- IP address of the C-LAN circuit pack Ethernet interface
- Port number of the C-LAN circuit pack Ethernet interface where adjunct connects

Setting up HyperTerminal on the computer

Use the HyperTerminal software program that comes with Windows NT/2000 to administer the IOLAN+.

1. Open HyperTerminal.
2. Click **File > Properties > Connect** tab. In the **Connect using:** field, select **COM *n***, where *n* is the communication port your computer is using.
3. Click **CONFIGURE** and set the **bits per second** field to **9600** and the **Flow control** field to **Hardware**.
4. Click **OK**.
5. Press **Enter** to get the log-in prompt.

Navigating the IOLAN+ terminal server

For more information, see the IOLAN+ user guide. Usually, you follow these steps:

- Use the arrow keys to move to a menu item.
- Use the **TAB** key to move from field to field horizontally.
- Use the **Enter** key to choose an item.

Administering the IOLAN+ the first time

1. At the login prompt, type **any text** and press **Enter**.

Adjuncts and peripherals

- At the second prompt, type **set term ansi** and press **Enter** to view the Connections menu.

```
Name: port 2                                CONNECTIONS MENU                                Terminal: 2

      Connection      Host

      1                *** FREE ** === Commands ===
      2                *** FREE ** | Telnet      ^T|
      3                *** FREE ** | Rlogin      ^R|
      4                *** FREE ** | Port        ^P|
                                | Admin mode ^A|
                                | CLI          |
                                | Lock         |
                                | Logout      ^D|
                                =====

IOLAN PLUS v4.02.00 a CDi                                iolan
```

- In **Connection** column, select **Port 1**, which is the port to which the adjunct is connected, and press **Enter**. You can now access the Commands menu.

4. Select **Admin mode > Password** and press **Enter**.

Name: port 2	ADMINISTRATION MENU	Terminal: 2
 gateway Examine/modify gateway table. host Examine/modify host table. line Terminal configuration organised by line. password Specify password to allow modification of menu items. port Terminal configuration organised by port. quit Return to connections menu. server Examine/modify Server parameters. stats Examine Server statistics. Password [] <hr/>		
IOLAN PLUS v4.02.00 a CDi		iolan-st

5. Type **iolan**, the default password, and press **Enter**.

The Administration Menu changes, offering more options.

6. Select **server** and press **Enter** to view the Server Configuration menu.

** Administrator **		SERVER CONFIGURATION		Terminal: 2	
Name	[iolan]	Debug mode	[0]		
IP address	[123.45.67.89]				
Subnet mask	[222.222.0.0]				
Ethernet address	[00:80:d4:03:11:cd]	Ethernet interface	[AUTO]		
Language	[English]				
Identification	[]				
Lock	[Disabled]				
Password limit	[5]				
CR to initiate	[No]				
SNAP encoding	[Disabled]				
Boot host	[]	Boot diagnostics	[Enabled]		
Boot file	[]				
Init file	[]				
MOTD file	[]				
Domain name	[]				
Name server	[]	NS Port	[53]		
WINS server	[]				

Name used for prompts and message on bottom right of screen.

IOLAN PLUS v4.02.00 a CDi iolan

7. Fill in the following fields with information appropriate to your network. Leave the default settings for the other fields.

- **Name:**
- **IP address:** (for IOLAN+)
- **Subnet mask:**

8. Press **Enter** and select **Save & Exit** to effect the changes.

Rebooting the IOLAN+

You must reboot the server any time you change an IP address or Local Port value.

1. Press **Enter** to view the Administration Menu.

```

** Administrator **                ADMINISTRATION MENU                Terminal: 2

access      Remote System Access (PPP).
change      Change login and/or admin password.
gateway     Examine/modify gateway table.
host        Examine/modify host table.
kill        Kill TCP connections on serial line.
line        Terminal configuration organised by line.
port        Terminal configuration organised by port.
quit        Return to connections menu.
reboot     Reboot Server.
server      Examine/modify Server parameters.
stats       Examine Server statistics.
trap        Examine/modify SNMP Trap parameters.

Port                [2 ]

IOLAN PLUS v4.02.00 a CDi                iolan

```

Note:

The following steps reinitialize the IOLAN+. The IOLAN+ is now connected to the LAN through the IP address.

2. Select **reboot** and press **Enter**.
3. Press the space bar to restart the IOLAN+.

Administering the gateway**Note:**

If the C-LAN circuit pack or S8300D Server and IOLAN+ are in the same subnet, skip the following steps.

1. Select **Admin mode > Password** and press **Enter**.
2. Type **iolan** and press **Enter**.
3. Select **gateway** to access the Gateway menu.
4. Fill in the following fields for Entry 1:
 - **Destination:** C-LAN or S8300D Server IP address
 - **Gateway:** Gateway address
 - **Netmask:** Subnet mask

Note:

The following steps reinitialize the IOLAN+. The IOLAN+ is now connected to the LAN through the gateway.

5. Select **reboot** and press **Enter**.
6. Press the space bar to restart the IOLAN+.

Administering an IOLAN+ port

Use this procedure for connecting an adjunct or serial COM port on a PC directly to the IOLAN+. See [Figure 11: Connecting an adjunct to the IOLAN+](#) on page 70.

1. Select **Admin mode > Password** and press **Enter**.
2. Type **iolan** and press **Enter**.
3. Select **port** and press **Enter**.
4. Type **port number**, where **port number** is the port that the adjunct connects to, and press **Enter** to view the Port Setup Menu.

** Administrator **		PORT SETUP MENU		Terminal: 2	
Hardware		Flow ctrl		Keys	
Speed	[9600]	Flow ctrl	[xon/xoff]	Hot	[^]] Intr [^C]
Parity	[None]	Input Flow	[Enabled]	Quit	[^@] Kill [^U]
Bit	[8]	Output Flow	[Enabled]	Del	[^@] Sess [^@]
Stop	[1]			Echo	[^@]
Break	[Disabled]	IP Addresses			
Monitor DSR	[Yes]	Src	[]	Mask	[]
Monitor DCD	[No]	Dst	[]		
User		Options		Access	
Name	[port 2]	Keepalive	[No]	Access	[Remote]
Terminal type	[undef]	Rlogin/Telnet	[Telnet]	Authentication	[None]
TERM	[]	Debug options	[No]	Mode	[Raw]
Video pages	[0]	Map CR to CR LF	[No]	Connection	[None]
CLI/Menu	[CLI]	Hex data	[No]	Host	[]
Reset Term	[No]	Secure	[No]	Remote Port	[0]
		MOTD	[No]	Local Port	[5101]
<hr/>					
IOLAN PLUS v4.02.00 a CDi				iolan	

5. Fill in the following fields. Leave the default settings for the other fields.

- **Speed: 9600**
- **Monitor DSR: Yes**
- **Monitor DCD: No**

- **Name:** Port number or other descriptive name
 - **Terminal type:** undef
 - **CLI/Menu:** CLI
 - **Reset Term:** No
 - **Flow ctrl:** xon/xoff
 - **IP addresses:** Leave blank
 - **Mask:** Leave blank
 - **Access:** Remote
 - **Authentication:** None
 - **Mode:** Raw
 - **Connection:** None
 - **Host:** Leave blank or enter the IP address of the C-LAN or S8300D Server
 - **Remote Port:** 0
 - **Local Port:** Must match the value of **Remote Port on the IP Services** screen of the Communication Manager software.
6. Press **Enter** and select **Save & Exit** to effect the changes.
 7. Press **Enter** again to view the Administration Menu.
 8. Select **kill** to disable the port connection.
 9. Repeat the steps for each additional port you want to administer.
 10. When administration is complete, from the Connections Menu, select **logout** or press **Ctrl D**.
 11. Close HyperTerminal.
- At this point, you have established a connection path from the adjunct through the IOLAN+ to the C-LAN circuit pack or S8300D Server.

Testing

1. On the system management terminal, press **Enter** to obtain the log-in prompt to the Communication Manager switch.

Note:

If you get garbled text, check the baud rate setting on the Port Setup Menu. You can adjust the setting up or down.

2. If the system does not display the log-in prompt, log back in to the IOLAN+ through HyperTerminal.
3. Select **Admin mode > stats** and press **Enter** twice.
4. Select **users** and press **Enter**.

Adjuncts and peripherals

5. Check the port that the adjunct is connected to for traffic. In the absence of traffic, check all your connections and administration fields.

```
** Administrator **          SERVER STATISTICS          Terminal: 2
1. port1                    Talking to host 172.22.22.67.5111<DSR+CTS+DCD >DTR+RTS
2. port 2                    SERVER STATISTICS              <DSR+DCD >DTR+RTS
3. port 3                    waiting for DSR or DCD          >DTR+RTS
4. port 4 modem              waiting for DSR or DCD          >DTR+RTS
REM <unknown>                logged out
LOG                           logger not enabled

Press <RETURN> to see list of options.
IOLAN PLUS v4.02.00 a CDi                                           iolan-st
```

You have now successfully administered and validated the connection between the adjunct and the C-LAN circuit pack or S8300D Server through the IOLAN+. Disconnect the laptop or other PC from the IOLAN+. No further IOLAN+ administration is required.

Potential failure scenarios and repair actions

If a link between the terminal server and the switch is disrupted, reboot the terminal server to connect. If you are performing a software upgrade or if a system reset occurs, you must reboot the terminal server to restore the link. For more information, see [Rebooting the IOLAN+](#) on page 74.

Administering IP node names

You must administer the IP addresses of all of the following components:

- the C-LAN board
- any adjunct that connects directly to the LAN
- the terminal server, if appropriate
- the PC that runs the Reliable Session-Layer Protocol, if appropriate

Use the **Node Names** screen to administer the IP addresses.

1. Type **change node-names ip** and press **RETURN**.

2. Type the name and the IP address of the C-LAN board and any adjunct, terminal server, or PC you must administer.
3. Print a copy of this screen, or write down the node names you entered. You need this information for the next administration task.
4. Press **Enter** to save your changes.

Administering IP services

For each adjunct that you connect using TCP/IP, you need to administer IP services to establish the IP address/TCP port pairing. The IP address is associated with the node name that you just administered. The following example is about administering the primary CDR connection as end-to-end TCP/IP and the PMS connection through a terminal server.

1. Type **change ip-services** and press **RETURN** to assign the CDR endpoint.
2. In the **Service Type** field, type **CDR1** for the call accounting link, and **PMS** for the property management system.
3. In the **Local Node** field, type the node name for the switch. In this example, **switch-clan** is the local node.
4. The default value for the **Local Port** field is **0** for all client applications. You cannot make an entry in this field.
5. In the **Remote Node** field, type the node name for the adjunct as administered on the **Node Names** screen. For the call accounting application, type **callacctg**. Since the PMS application routes through the terminal server, **termserver** is the remote node for this service type.
6. In the **Remote Port** field, type the TCP listen port assigned to the adjunct. The recommended value for CDR1 is **5101**, and the recommended value for PMS is **5103**.

Note:

This number must match the port administered on the end device. If you are using the Downloadable Reliable Session-Layer Protocol tool, this number must match the port administered in the Server application. If you are using a terminal server, this number must match the Local Port number on the Port Setup menu. Consult the document for your Call Accounting system to determine the appropriate port for the CDR device.

7. Move to Page 3. In the **Reliable Protocol** field, type **n** for the CDR Service Type. You do not use RSP with a terminal server.
8. Press **Enter** to save your changes.

Call detail recording

This section provides information on connecting the call detail recording (CDR) equipment.

Connecting CDR Equipment

The interface between an Avaya server and the CDR equipment is a C-LAN card or Processor Ethernet Connection.

CDR equipment connects to the C-LAN circuit pack in a G650 Media Gateway through a TCP/IP connection which is an Ethernet connection. Any CDR equipment that supports the Reliable Session Protocol supports a direct TCP/IP connection. A CDR application that supports an RS232 interface can also connect to the C-LAN through a terminal server. For more information about connecting through a terminal server, see [Terminal server installation](#) on page 67.

CDR equipment connects to one of the two IP connections (EXT 1 or EXT 2) on the front of the G700 or G350 Branch Gateway. As with C-LAN connections, the CDR adjunct may be a terminal server or a CDR application using RSP.

Note:

You can also use a printer or customer premises equipment (CPE) as the output receiving device. For more information about using a printer, see [Terminal server installation](#) on page 67.

Administering CDR data collection

The following steps administer the CDR data collection.

Note:

To send CDR data through the C-LAN or a processor Ethernet interface to a device on the LAN/WAN, you have the option to enable/disable RSP.

1. Set up the CDR adjunct to be ready to collect CDR data. Record the IP address and the port number of the CDR adjunct, which can be a terminal server or a CDR application that uses RSP.

If the CDR adjunct is an application that uses RSP, start the application to listen for a client connection at the port.

2. Access the **Node Names** screen in Communication Manager. For more information, see [Administering IP node names](#) on page 78. Perform the following steps:
 - a. In the **Name** field, type the name of the CDR adjunct from Step 1.

- b. In the **Address** field, type the IP address of the CDR adjunct.
3. Access the **IP Services** screen in Communication Manager. For more information, see [Administering IP services](#) on page 79. Perform the following steps:
 - a. In the **Service Type** field, type CDR1 or CDR2.
 - b. In the **Local Node** field, type `switch-clan` or `procr`.
 - c. The default value for the **Local Port** field is **0** for all client applications. You cannot make an entry in this field.
 - d. In the **Remote Node** field, type the node name you assigned to the CDR adjunct in step 2.
 - e. In the **Remote Port** field, type the port number used by the CDR adjunct determined in step 1.
4. Go to Page 3 and perform the following steps:
 - a. In the **Reliable Protocol** field, type **y** if you have a CDR application using RSP. Type **n** if the CDR adjunct is connected through a terminal server.
 - b. If RSP is being used, complete the **Packet Resp Timer** and **Connectivity Timer** fields with some reasonable value that matches the network condition. The recommended values are **30** and **60** seconds, respectively.
 - c. Leave the defaults in the other fields.
5. Administer CDR parameters as described in [Administering CDR parameters](#) on page 81.

Administering CDR parameters

You must administer CDR parameters to apprise the system that the adjunct is connected through TCP/IP. For more information about all fields on the **CDR System Parameters** screen, see *Administering Avaya Aura® Communication Manager*, 03-300509.

1. Type `change system-parameters cdr` and press **ENTER**.
2. In the **Primary Output Format** field, type a format specific to the call accounting system, if necessary. In the example, **unformatted** is used. If you are sending data directly to a printer, you use **printer**.
3. In the **Primary Output Endpoint** field, type CDR1.
4. If you use a secondary output device, and that device is also connected through TCP/IP, complete the **Secondary Output Format** field. Also, type CDR2 in the **Secondary Output Endpoint** field.
5. Press **Enter** to save your changes.

Testing the switch-to-adjunct link

You can use the `test`, `status`, `busyout` and `release` commands to find and correct problems with CDR links. For more information about these commands, see the Maintenance manual for your switch.

Work with the vendor to test the link from the call accounting adjunct.

If a link does not come up immediately, use the `busyout cdr-link` and `release cdr-link` commands to display the link if the link does not display immediately.

For additional administration procedures for CDR equipment, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Reliable Data Transport Tool package

Avaya provides this free software application to help vendors and customers develop CDR applications. These applications use the reliable session protocol to collect CDR data from an Avaya server. The Reliable Data Transport Tool (RDTT) is a testing tool. Therefore, Avaya does not support the RDTT.

Contents of the RDTT

The RDTT package consists of the following components:

- Specifications for the Reliable Session Protocol
- The Client application (Client.exe)

With this application, you can test the reliable session protocol without use of an Avaya server.

- The Server application (Server.exe)

With this application, you can understand the reliable session protocol and start building your products to work with the Avaya server.

- User Guide

This document contains information about the client and server applications.

Downloading RDTT

The RDTT tool is available from the Avaya Support Web site as a self-extracting executable. To download the RDTT:

1. Log on to <http://support.avaya.com>.
2. In the **InSite Knowledge Base** search box, type **Reliable Data Transport Client/Server Tool** including the quotation marks.
3. Press **Enter**.
4. In the search results, click the appropriate Communication Manager Downloads link of 08/26/2010.
5. On the download page, click **Reliable Data Transport Client/Server Tool V2.0 of 31-Aug-2005**.
6. Click **RDTT_R2.1.exe**.
7. Click **Save**.
8. Make note of the default download directory or browse to the appropriate directory.
9. Click **Save**.
10. Click **Run**.

Note:

To view and save the accompanying ReadMe file, select **RDTT_Readme_2.1.doc**.

Installing RDTT

To install the RDTT:

1. Double-click the **RDTT.exe** file.
The Install Shield Wizard guides you through the installation.
2. When prompted to select Client or Server, select both programs.
3. Continue with the installation. Use the default destination folder and program folder.

Administering RDTT

See the instructions in the `user_guide.doc` file to administer the RDTT tool on a PC.

Related topics

For more information about the CDR-related sections, see:

- Chapter 17, “Collecting Billing Information,” in *Administering Avaya Aura® Communication Manager*, 03-300509.
- “Call Detail Recording” in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.
- [Connecting printers using TCP/IP](#) on page 92.

Wideband endpoints

Wideband endpoints include video equipment or bridges/routers for LANs. Use the running list that accompanies the system to make cable connections.

Nonsignaling configuration

A nonsignaling connection to a wideband endpoint might connect to a channel service unit (**CSU**). If *not* using a **CSU**, the distance between the system and the endpoint is limited to a few hundred feet. See [Figure 12: Typical nonsignaling wideband configuration](#). The maximum distance depends on the type of cable and type of endpoint.

Figure 12: Typical nonsignaling wideband configuration

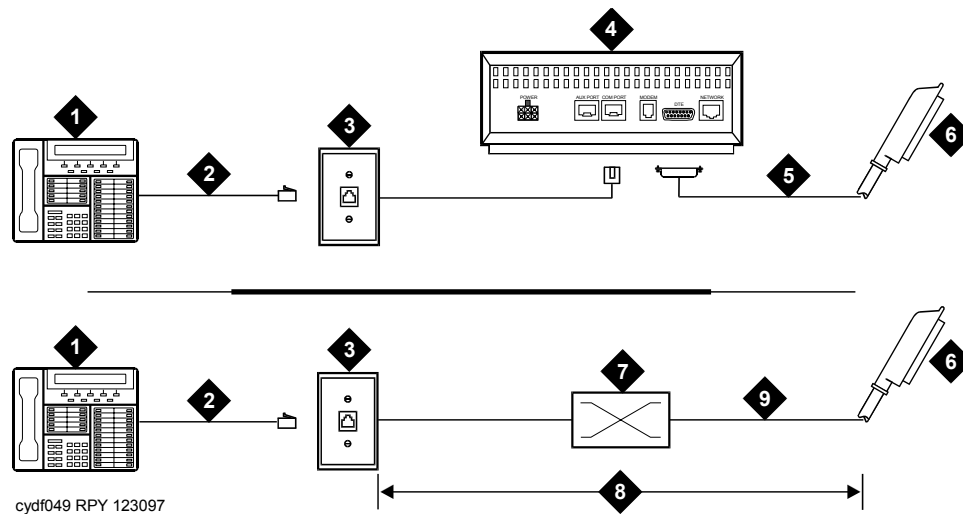


Figure notes:

- | | |
|--|---|
| 1. Wideband endpoint (wire per manufacturer) | 6. DS1/E1 circuit pack |
| 2. Modular cord | 7. Main distribution frame (MDF) |
| 3. 103A or modular wall jack | 8. Distance limit that depends on cable and endpoint type |
| 4. Channel service unit (CSU) | 9. A25D 25-pair cable (male-to-male) |
| 5. H600-307 cable to DTE connector on CSU | |

If using a **CSU**, the distance between connections can be up to 1300 ft. (397.2 m). The maximum distance to the endpoint depends on the type of cable and the specifications of the endpoint.

Signaling configuration

A signaling connection from the system to a wideband endpoint passes through a bandwidth controller. The distance between the system and the bandwidth controller depends on the type of cable and controller. [Figure 13: Typical signaling wideband configuration](#) shows connections with and without a CSU.

Figure 13: Typical signaling wideband configuration

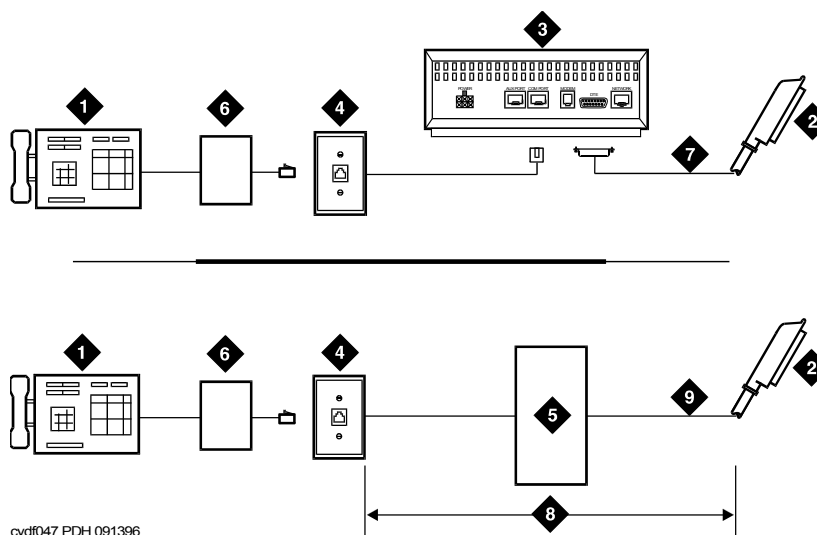


Figure notes:

- | | |
|--|--|
| 1. Wideband endpoint (wire per manufacturer) | 6. Bandwidth controller |
| 2. To DS1/E1 circuit pack | 7. H600-307 cable to DTE connector on CSU |
| 3. Optional channel service unit (CSU) | 8. Distance limit that depends on cable type and bandwidth controller type |
| 4. 103A or modular wall jack | 9. A25D 25-pair cable (male-to-male) |
| 5. Part of main distribution frame | |

The bandwidth controller connects directly to the wideband endpoint as the controller is located near the endpoint, usually within a few feet of each other.

- For non-CSU installations, cross the transmit and receive lines. Through these crossed lines, a transmit signal from the DS1/E1 circuit pack connects to the receive connection on the bandwidth controller. In addition, a transmit signal from the bandwidth controller connects to the receive connection on the DS1/E1 circuit pack.
- For CSU installations, cross the transmit and receive lines between the CSU and the bandwidth controller.

[Figure 14: Typical signaling wideband configuration with remote port module](#) shows a remote port module. In this configuration, the distance between the bandwidth controller and the

wideband endpoint is considerable. The maximum distance between elements depends on the quality of the cables and on the specifications of the wideband equipment.

Figure 14: Typical signaling wideband configuration with remote port module

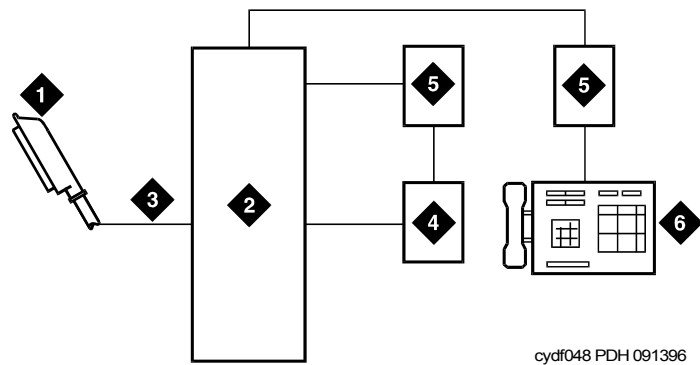


Figure notes:

- | | |
|--|--|
| 1. To TN464F DS1/E1 circuit pack | 4. Bandwidth controller |
| 2. Part of main distribution frame (MDF) | 5. Remote port module |
| 3. H600-307 cable | 6. Wideband endpoint (wire per manufacturer) |

-
1. For non-CSU installations, cross the transmit and receive lines. Through these crossed lines, a transmit signal from the TN464F connects to the receive connection on the bandwidth controller. In addition, a transmit signal from the bandwidth controller connects to the receive connection on the TN464F.
 2. For CSU installations, cross the transmit and receive lines between the CSU and the bandwidth controller.
-

Multimedia call handling

Multimedia call handling (MMCH) provides a single point-to-point conference call using voice, video, and data from one endpoint to another. You must have endpoints and a personal computer with H.320 desktop video installed.

Connecting the endpoints

Use the following procedure and [Figure 15: Typical multimedia call handling connections](#) to connect the endpoints:

Figure 15: Typical multimedia call handling connections

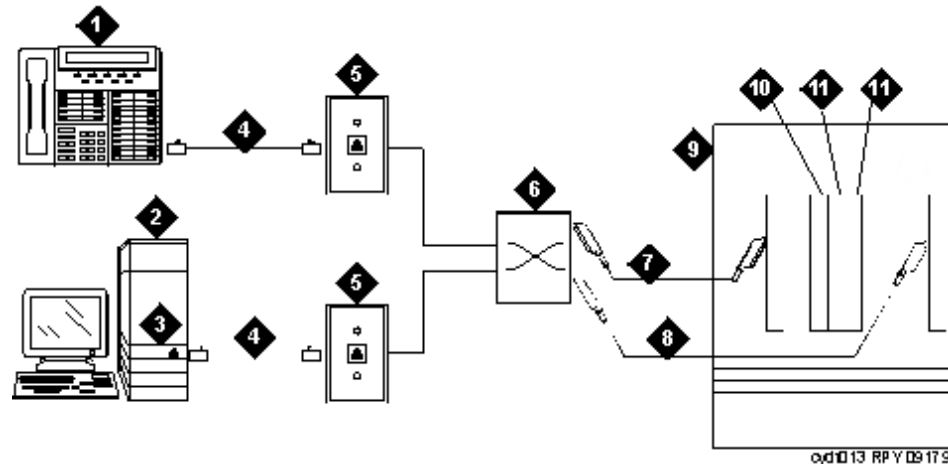


Figure notes:

- | | |
|---|--|
| 1. DCP telephone, 2 or 4 wire to match type of circuit pack | 7. 25-pair cable to digital line circuit pack |
| 2. Personal computer | 8. 25-pair cable to BRI circuit pack or NT1, 4-to-2 wire adapter |
| 3. BRI adapter | 9. Avaya server |
| 4. D8W cord | 10. Multimedia interface circuit pack |
| 5. 103A or modular wall jack | 11. Voice conditioner circuit pack |
| 6. Main distribution frame | |

1. Each PC MMCH endpoint must contain a BRI adapter.
2. Connect a DCP telephone to a digital line circuit pack. Use the DCP telephone in conjunction with the PC. For more information on the pinout of the digital line circuit pack, see the tables at the end of this chapter.
3. Connect the PC BRI adapter to any BRI port on the Avaya server. For the pinout of an ISDN BRI circuit pack, see the tables at the end of Chapter 5.

Administering the system

The following steps administer the system.

1. Call INADS and notify the representative to change the **Multimedia Call Handling (MMCH)?** field on page 2 of the **System-Parameters Customer-Options** screen to **y**.
2. Log off the terminal and then log back on the terminal to see your changes.

Administering the endpoints

The following steps administer the endpoints.

1. Log in and type **add data-next** <or a valid extension number>.
2. The system displays the **Data Module** screen. On page 1:
 - In the **Data Extension:** field, type **xxxx**.
 - In the **Type:** field, type **7500**.
 - In the **Name:** field, type the user name, such as ProShare.
 - In **Multimedia?** field, type **y**.
3. On page 2:
 - In the **XID?** field, type **n**.
 - In the **MIM Support?** field, type **n** and press **Enter**.

Administering one number complex

The following steps administer the one number complex.

1. Identify the voice telephone (DCP set) to associate with the data endpoint. Change the station record for this voice station.
2. Type **change station station number** and press **Enter**.
3. On screen 1, in the **MM Complex Data Ext:** field, type the data extension number.
4. On screen 2, in the **H.320 Conversion?** field, type **y** and press **Enter**.
5. In the **Multimedia Early Answer** field, type **y** and press **Enter**.

Expansion services module

The Expansion Services Module (ESM) provides T.120 data sharing capability on a MMCH multipoint H.320 video conference. Each person in the conference must have endpoints and a personal computer with the H.320 video application installed. The Avaya server must have the expansion service module installed.

Figure 16: Typical multimedia call handling ESM connections

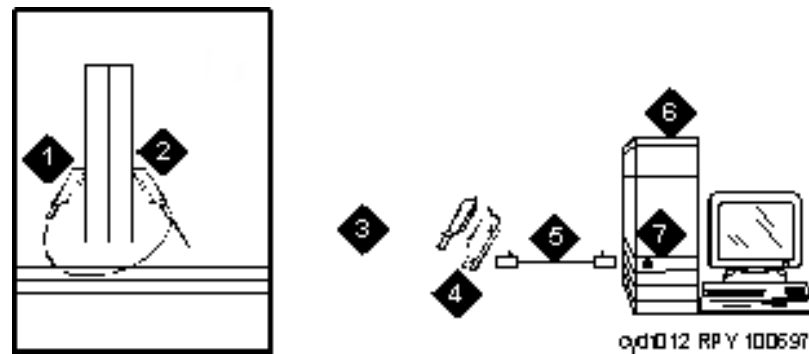


Figure notes:

1. Port B Y-cable connector to a TN787 multimedia interface (MMI) circuit pack
2. Port A Y-cable connector to a TN2207 PRI circuit pack
3. 25-pair Y-cable
4. 357A adapter
5. D8W cord connected to 357A adapter S/B port 8
6. Expansion service module (ESM)
7. Port B on compatible primary rate interface (PRI) card

ESM installation

Use the following procedure and [Figure 16: Typical multimedia call handling ESM connections](#) on page 90 to connect to the ESM equipment:

1. Install the TN2207 primary rate interface (PRI) circuit pack and the TN787F/G/H/J/K multimedia interface (MMI) circuit pack in the port carrier.
2. Record the circuit pack locations.
3. Connect the ESM Y-cable as shown.

Administration

The following steps administer the DS1 circuit packs.

1. Type `list configuration all` and press **Enter**.

The system displays a list of the installed carriers, circuit packs, and ports.

2. Record the board number location of the new circuit packs and verify that all other required circuit packs are present. For more information on this procedure, see [ESM installation](#) on page 90.

3. Type **add DS1 *xxxxxx*** where ***xxxxxx*** is the location of the TN2207 PRI circuit pack recorded in step 2 and press **Enter**.

The system displays the DS1 circuit pack administration form.

4. Set the **Name:** field to **ESM DS1**.
5. Set the **Bit Rate:** field to **2.048**.
6. Set the **Line Coding:** field to **hdb3**.
7. Set the **Signaling Mode:** field to **isdn-pri**.
8. Set the **Connect:** field to **pbx**.
9. Set the **Interface:** field to **network**.
10. Set the **Country Protocol:**field to **1**.
11. Set the **Protocol Version:**field to **a**.
12. Set the **CRC?:**field to **y**.
13. The Idle Code default is 11111111.
14. The DCP/Analog Bearer Capability default is 3.1 kHz.
15. Set the **MMI Cabling Board:** field to ***xxxxxx*** where ***xxxxxx*** is the location of the TN787F/H/J/K MMI circuit pack recorded in step 2. Ensure that this location is the slot for port B of the Y-cable.

The system displays the **MMI Interface:** field **ESM**.

16. Type **add signaling-group next**.

The system displays the signaling-group form.

17. Change **Associated Signaling:** field to **y**.
18. Change **Primary D-Channel Port:** field to ***xxxx*17** where ***xxxx*** is the address of the TN2207 PRI circuit pack. An example address is B0517.
19. The **Max Number of NCA TSC:** default is 0.
20. The **Max Number of GA TSC:** default is 0.
21. **Trunk Group for NCA TSC:** ____ (leave blank).
22. **Trunk Group for Channel Selection:**____ (leave blank).
23. Log off the terminal and then log back on the terminal to view your changes.

Place test call

Place multimedia data-conference call to an endpoint with known video capability to test the esm function.

Troubleshooting

To determine the ESM link status, type the following commands from the system administration terminal:

- **Status esm**
- **Status signaling-group**
- **List MMI**

Note:

When you move ESM circuit packs, you must remove the DS1 and signaling group translations. You cannot use the **change circuit pack** command.

For more information, see [Expansion services module](#) on page 89.

Printers

This section provides information on connecting and configuring printers that work with your system and Communication Manager.

Connecting printers using TCP/IP

You can connect printers to the switch using asynchronous TCP/IP links and a terminal server. This section provides information on connecting adjuncts to the C-LAN circuit pack in a branch gateway. This section also provides the initial administration for these connections. For more information on connecting a printer to a G700 or G350 Branch Gateway, see [Terminal server installation](#) on page 67.

Task list

Whether you use an end-to-end TCP/IP configuration, a terminal server, or a PC running RSP, you must complete the following tasks:

- [Administering IP node names](#) on page 78
- [Administering IP services](#) on page 79
- [Administering adjunct parameters](#) on page 93
- If you are using a terminal server, also complete [Installing and administering the terminal server](#) on page 68

- If you are using a PC with the Downloadable RSP Tool, complete [Using the downloadable reliable session-layer protocol \(RSP\) tool](#) on page 93.

Administering adjunct parameters

You must administer adjunct parameters to apprise the system that the adjunct is connected through TCP/IP.

PMS journal and PMS log printers

See *Guestworks and DEFINITY Systems Technician Handbook for Hospitality Installations*, 555-231-743.

System printer

1. Type **change system-parameters features** and press **Enter**.

The system displays the **Feature-Related System Parameters** screen.

2. Move to Page 4.
3. In the **System Printer Endpoint** field, type **SYS_PRNT**.
4. Press **Enter** to save your changes.

Testing the switch-to-adjunct link

You can use the test, status, busyout, and release commands to find and correct problems with a system printer, PMS log printer, or PMS journal printer. For more information about these commands, see the Maintenance manual for your switch.

If a link does not display immediately, use the busyout and release commands. The busyout commands are journal-link pms-log and wakeup-log, and sp-link. The release commands are journal-link pms-log and wakeup-log, and sp-link.

Note:

Status sp-link can falsely show a system printer link as nonfunctional. If no data is being transmitted, the switch might not see this link as active.

Using the downloadable reliable session-layer protocol (RSP) tool

The intent of the Reliable Session-Layer Protocol (RSP) is to guarantee delivery of data records from the switch. The protocol delivers the records to an output device that connects to the switch over an asynchronous TCP/IP link. With the Downloadable RDTT tool, you can implement this protocol on a PC that collects data records in a file. The protocol ensures that the data records arrive safely at the PC. You can then send the output file to a printer. For more information, see [Reliable Data Transport Tool package](#) on page 82.

DS1/T1 CPE loopback jack

This section provides information on how to install and use a DS1 loopback jack. You can use the jack to test the DS1 span between the Avaya server or gateway and the network interface point. The loopback jack is required when DC power is at the interface to the integrated channel service unit (ICSU).

Note:

Do not remove the loopback jack after installation. The jack must always be available for remote tests of the DS1 span.

Note:

For G700 or G350 Branch Gateway systems, the channel service unit (CSU) is integrated within the MM710 board and you do not need a separate external device. For earlier branch gateway systems, the integrated channel service unit (ICSU), also known as the 120A2, is a separate device. The ICSU plugs into the back of the branch gateway.

Note:

For G700 or G350 Branch Gateway systems, the loopback jack isolates the MM710 internal CSU from the DC power and properly loops the DC span power.

Installing a loopback jack

You can install a loopback jack with or without a smart jack.

With a smart jack

Install the loopback jack at the interface to the smart jack, if possible. This position provides maximum coverage of CPE wiring when remote loopback tests are run. The installation method depends on whether the smart jack is accessible and whether there is an extended demarcation point. The following installation scenarios are possible.

- 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. For an example of this installation, see [Figure 17: Network interface at smart jack for a 120A2 \(or later\) ICSU](#) on page 104.
- If there is an extended demarcation point and the smart jack is not accessible, install the loopback jack as shown in [Figure 18: Network interface at extended demarcation point \(smart jack inaccessible\) for a 120A2 \(or later\) ICSU](#) on page 105.

- If there is an extended demarcation point, but the smart jack is accessible, install the loopback jack as shown in [Figure 19: Network interface at extended demarcation point \(smart jack accessible\) for a 120A2 \(or later\) ICSU](#) on page 106.

To install the loopback jack:

1. Disconnect the RJ-48 (8-wide) connector at the appropriate interface point and connect the loopback jack in series with the DS1 span. For examples, see [Figure 17: Network interface at smart jack for a 120A2 \(or later\) ICSU](#) on page 104 through [Figure 21: Network interface at “dumb” block with repeater line to fiber MUX for a 120A2 \(or later\) ICSU](#) on page 108.
2. Plug the H600-383 cable from the ICSU or the MM710 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. The jack is not a test tool and must always be available to remotely test a DS1 span.

Without a smart jack

Install the loopback jack at the point where the cable connections 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 choice provides maximum coverage for loopback jack tests. See [Figure 20: Network interface at “dumb” block for a 120A2 \(or later\) ICSU](#) on page 107 and [Figure 21: Network interface at “dumb” block with repeater line to fiber MUX for a 120A2 \(or later\) ICSU](#) on page 108.

To install the loopback jack:

1. Disconnect the RJ-48 (8-wide) connector at the appropriate interface point and connect the loopback jack in series with the DS1 span. For examples, see [Figure 17: Network interface at smart jack for a 120A2 \(or later\) ICSU](#) on page 104 through [Figure 21: Network interface at “dumb” block with repeater line to fiber MUX for a 120A2 \(or later\) ICSU](#) on page 108.
2. Plug the H600-383 cable from the ICSU, or from the MM710, 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. The jack is not a test tool and must always be available to remotely test a DS1 span.

Administering the loopback jack

The following steps administer the loopback jack.

1. At the management terminal, type **change ds1 location** where **location** is the DS1 interface circuit pack that corresponds to the loopback jack. Press **Enter**.
2. Verify that 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**.

When you set this field to **y**, the system informs the technician that a loopback jack is present on the facility. The technician can determine whether the facility is available for remote testing.

4. Type **save translation** and press **Enter** to save the new information.

Loopback testing with a smart jack

The loopback jack and the smart jack isolate faults by dividing the DS1 span into three sections. For more information, see [Figure 17: Network interface at smart jack for a 120A2 \(or later\) ICSU](#) on page 104 through [Figure 19: Network interface at extended demarcation point \(smart jack accessible\) for a 120A2 \(or later\) ICSU](#) on page 106.

The three sections are:

- From the 120A2, or later, ICSU, or from the MM710 to the loopback jack
- From the loopback jack to the smart jack, which is the network interface point
- From the smart jack to the CO

You must perform the first two sections. The last is the responsibility of the DS1 service provider.

Testing the DS1 span from the ICSU to the loopback jack

The DS1 span test has two parts.

- Checking for circuit connectivity

The first part of the test turns on power to the loopback jack. The test sends a signal from the DS1 circuit pack, through the wiring, to the loopback jack. The test allows about 10 seconds for the signal to loop around the loopback jack and return to the DS1 circuit pack. Then the test sends the results to the management terminal and proceeds to the second part of the test.

- The second part of the test sends the standard, 3-in-24 DS1 stress-testing pattern from the DS1 board, through the loopback jack, and back to a bit error detector and counter on the

DS1 board. A bit-error rate counter displays the results on the management terminal until you terminate the test.

The following is the sequence of the test procedure:

- [Checking the integrity of local equipment](#)
- [Busying out the DS1 circuit pack](#)
- [Administering the DS1 for the test](#)
- [Testing the integrity of the loopback circuit](#)
- [Testing the integrity of data sent over the loop](#)
- [Clearing the results of previous tests](#)
- [Running the data test](#)

Checking the integrity of local equipment

Ensure that the problem is actually on the DS1 span by testing the equipment that connects to the span at the near end. Test the DS1 circuit pack, and perform any needed maintenance or repairs.

Busying out the DS1 circuit pack

Now take the DS1 circuit out of service.

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uucss** in the following command. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and must be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

- Once you are sure that the DS1 circuit pack and ICSU are functioning correctly, go to the management terminal and busy out the DS1 circuit pack by typing **busyout board uucss**, where **uu** is the cabinet number, **c** is the carrier letter, and **ss** is the slot number of the DS1 board.

Administering the DS1 for the test

1. At the management terminal, open the **DS1 Administration** screen. Type **change ds1 uucss**, where **uu** is the cabinet number, **c** is the carrier letter, and **ss** is the slot number of the DS1 board.
2. Ensure that the **near-end csu type** field is set to **integrated**.
3. On page 2 of the **DS1 administration** screen, confirm that the value of the **TX LBO** field is **0dB**.
4. If the value of the **TX LBO** field is not **0dB**, record the current value. Then set the **TX LBO** field to **0dB** for testing.

5. Press **Enter** to make the changes. Press **Cancel** to quit without making changes.

Testing the integrity of the loopback circuit

Now perform the first part of the actual loopback test.

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uucss** in the following command. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and you must include the V exactly where shown in the command. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway might look like this: 002V3.

1. At the management terminal, type **test ds1-loop uucss cpe-loopback-jack**. **uu** is the cabinet number. **c** is the carrier letter. **ss** is the slot number of the DS1 board.

The loopback jack turns on. Active, DS1 facility alarms (if any) clear. After about 20 seconds, the first set of results displays on the terminal.

2. If **FAIL** message on the terminal display indicates a fault in the the loopback jack or in the wiring between the ICSU and the loopback jack. To isolate the problem, replace the loopback jack and repeat Step [1](#).
3. If the terminal continues to display the **FAIL** message after you replace the loopback jack, the message indicates a wiring problem. Replace the cable between the ICSU and the loopback jack. Then repeat Step [1](#).
4. When the terminal displays a **PASS** message, proceed with the second part of the test and check the integrity of the transmitted data.

Testing the integrity of data sent over the loop

Now perform the second part of the test, checking for data errors.

Note:

The system does not process the loss of signal (LOS) alarm in demand test #138 during this test while the 3-in-24 pattern is active.

Clearing the results of previous tests

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uucss** in the following commands. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

1. Ensure that the bit-error counter is at zero. At the management terminal, type `clear meas ds1 loop UUCS`. *UU* is the cabinet number. *C* is the carrier letter. *SS* is the slot number of the DS1 board.
2. Ensure that the performance measurement counter is at zero. At the management terminal, type `clear meas ds1 log UUCS`. *UU* is the cabinet number. *C* is the carrier letter. *SS* is the slot number of the DS1 board.
3. Ensure that the ESF error count is at zero. At the management terminal, type `clear meas ds1 esf UUCS`. *UU* is the cabinet number. *C* is the carrier letter. *SS* is the slot number of the DS1 board.

Running the data test

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for *UUCS* in the following command. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

1. Display the bit-error count. At the management terminal, type `list meas ds1 sum UUCS`. *UU* is the cabinet number. *C* is the carrier letter. *SS* is the slot number of the DS1 board.
2. To troubleshoot, see [Table 9: DS1 Troubleshooting](#) on page 99.

Table 9: DS1 Troubleshooting

Condition	Solution
The value of the Test: cpe-loopback-jack field is Pattern 3-in-24 .	The loopback jack test is active.
The value of the Synchronized field is N .	Retry the test five times.
The value of the Synchronized field remains N after 5 attempts.	Excessive bit errors are likely. Check for intermittent connections or broken wires in an SPE receive or transmit pair, and repair as necessary. Then repeat step 1 .
The value of the Bit-error count field is non-zero .	Then repeat Step 1 several times.
The value of the Synchronized is Y .	The DS1 circuit pack has synchronized to the looped 3-in-24 pattern and is counting bit errors in the pattern.
1 of 2	

Table 9: DS1 Troubleshooting (*continued*)

Condition	Solution
The value of the Bit-error count field pegs at 75535 or increments by 100s or 1000s whenever you repeat step 1 .	Suspect loose or corroded connections, severe crosstalk, or impedance imbalances between the two conductors of the receive or transmit pair. Wiring might need replacement.
The value of the Bit-error count field is 0 .	Wiring problems are obvious, but repeat Step 1 at 1-minute to 10-minute intervals to verify. If the test reports no errors for 1 minute, the error rate is less than 1 in 10 ⁸ . If the test reports no errors for 10 minutes, the error rate is less than 1 in 10 ⁹ .
2 of 2	

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uuCSS** in the following commands. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

- If you have at least one error-free minute, you can assume that the test is reporting no errors. Then, confirm that the 3-in-24 pattern error detector is functional. Type **test ds1-loop uuCSS inject-single-bit-error**. **uu** is the cabinet number. **c** is the carrier letter. **ss** is the slot number of the DS1 board.
- Display the bit error count again. At the management terminal, type **list meas ds1 sum uuCSS**, where **uu** is the cabinet number, **c** is the carrier letter, and **ss** is the slot number of the DS1 board.

Condition	Solution
The value of the Bit-error count field is greater than 1 .	Replace the ICSU, and retest.
The value of the Bit-error count field is still greater than 1 after you replace the ICSU.	Replace the DS1 circuit pack, and retest.
The value of the Bit-error count field is 1 .	The system passes the test.

- To end the test, type **test ds1-loop location end cpe-loopback-jack-test**.

6. Wait about 30 seconds for the DS1 to reframe on the incoming signal and clear DS1 facility alarms.

Condition	Solution
Loopback termination fails with an error code of 1313.	The span is still looped somewhere, possibly at the loopback jack, at the ICSU, or somewhere in the network.
The red LED on the loopback jack is on.	Replace the ICSU, and rerun the test.
Loopback termination still fails.	Replace the DS1 circuit pack, and repeat the test.
The DS1 cannot frame on the incoming span signal after the loopback jack turns off.	There is something wrong with the receive signal into the loopback jack from the dumb block or the smart jack.
The span failed the loopback test for the service provider.	The problem is in the service provider network.
The service provider successfully loop tested the span, up to the smart jack.	The wiring between the loopback jack and the smart jack is suspect. Test and make repairs, as needed.
You cannot locate and repair the problem in the time available and must terminate the test.	The test does not terminate normally in the absence of a good framing signal. You have to reset the circuit pack. Type reset board <i>uu</i>css , where <i>uu</i> is the cabinet number, <i>C</i> is the carrier letter, and <i>SS</i> is the slot number of the DS1 board.
Note: If you have a G700 or G350 Branch Gateway, substitute <i>xxxvs</i> for <i>uu</i>css in the above command. <i>xxx</i> is the administered number of the G700 or G350, such as 002. <i>vs</i> is the slot number on the G700 or G350 of the Media Module, such as V3. The <i>v</i> is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.	
The test terminated normally.	Proceed with Restoring DS1 administration .

Restoring DS1 administration

To restore DS1 administration:

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uucss** in the following command. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

1. At the management terminal, open the **DS1 Administration** screen. Type **change ds1 uucss**, where **uu** is the cabinet number, **c** is the carrier letter, and **ss** is the slot number of the DS1 board.
2. On page 2 of the **DS1 Administration** screen, change the value of the **TX LBO** field to the original value that you wrote down when you administered the DS1 for the test. See [Administering the DS1 for the test](#) on page 97.
3. Press **Enter** to make the changes. Press **Cancel** to quit without making changes.

Releasing the DS1 circuit pack

To release the DS1 circuit pack:

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uucss** in the following command. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

1. To release the DS1 circuit pack, on the management terminal, type **release board uucss**, where **uu** is the cabinet number, **c** is the carrier letter, and **ss** is the slot number of the DS1 board.
2. Leave the loopback jack in place.

Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer (MUX)

The following steps test the DS1 span.

1. Request the service provider to run a smart-jack loopback test on the network interface wiring that links the smart jack to the CO. For more information, see section 3 in [Figure 17: Network interface at smart jack for a 120A2 \(or later\) ICSU](#) on page 104 through

[Figure 19: Network interface at extended demarcation point \(smart jack accessible\) for a 120A2 \(or later\) ICSU](#) on page 106.

2. A negative test result indicates a problem on the network side. Request the service provider to correct the problem.

Testing the DS1 span from the loopback jack to the smart jack

Test the short length of customer premises wiring between the loopback jack and the smart jack. Use a loopback that overlaps this section of the span.

For more information, see Span section 2 in [Figure 17](#), [Figure 18](#), and [Figure 19](#).

- Request the DS1 service provider at the CO end to run a local ICSU line loopback test and a local DS1 payload loopback test.
- To run a far-end ICSU or MM710 line loopback:

Note:

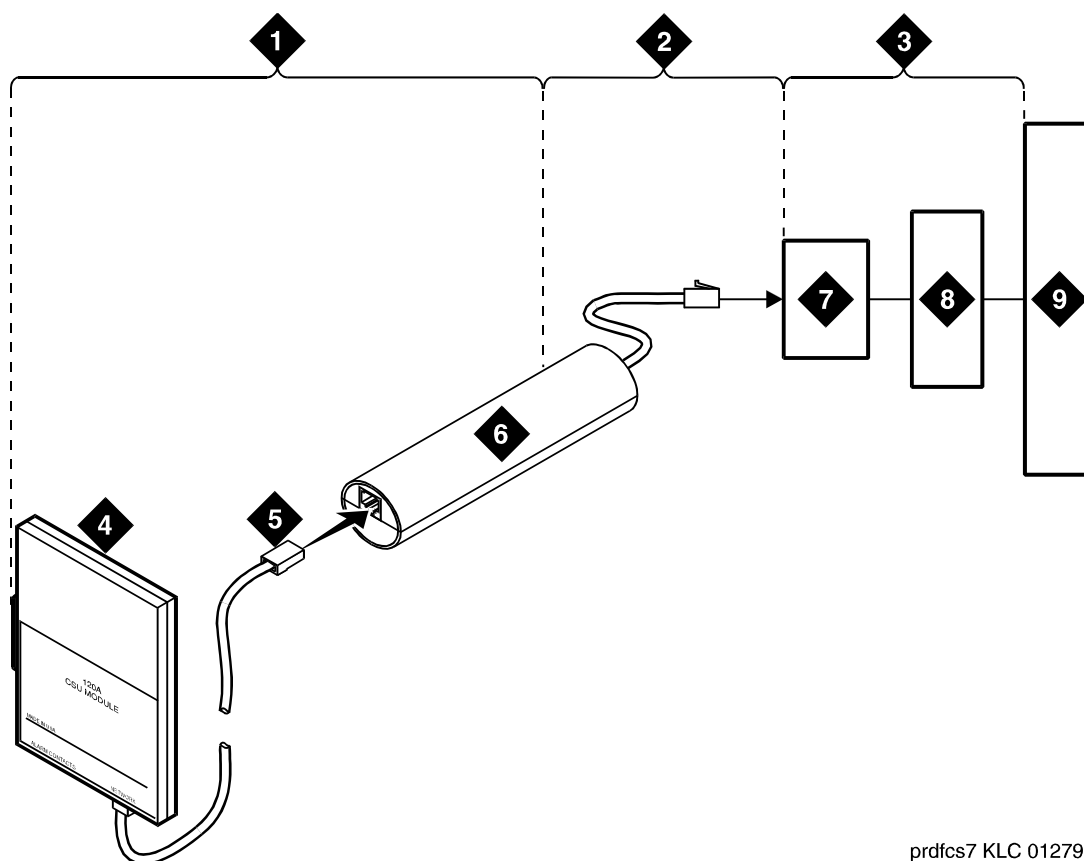
This test cannot isolate the problem if there are problems in the wiring between the far-end CO and the far-end ICSU. You must coordinate this test with the DS1 service provider.

Note:

If you have a G700 or G350 Branch Gateway, substitute **xxxvs** for **uucss** in the following command. **xxx** is the administered number of the G700 or G350, such as 002. **vs** is the slot number on the G700 or G350 of the Media Module, such as V3. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway is 002V3.

1. From the management terminal, type **test ds1-loop location far-csu-loopback-test-begin**, where *location* is the cabinet and slot location of the DS1 board (for example, 02205) or the administered and slot number of the G700. The **v** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Branch Gateway might look like this: 002V3.
2. Examine the bit-error counts, as in [Testing the integrity of data sent over the loop](#) on page 98.
3. Terminate the test, type **test ds1-loop location end-loopback/span-test**.
4. If the tests fails and no problems develop when you follow the procedures in [Testing the DS1 span from the ICSU to the loopback jack](#) on page 96 or [Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer \(MUX\)](#) on page 102, a problem might exist between the loopback jack and the smart jack. Work with the service provider to isolate the fault.

Figure 17: Network interface at smart jack for a 120A2 (or later) ICSU

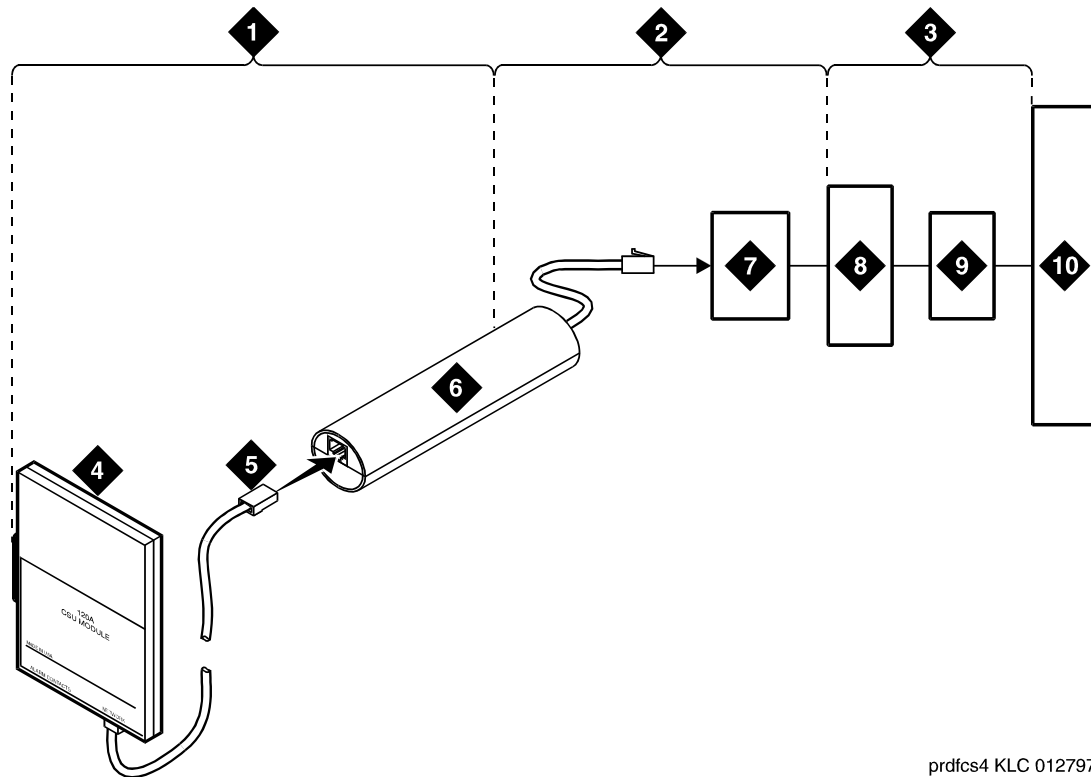


prdfcs7 KLC 012797

Figure notes:

- | | |
|--|---|
| 1. Span section 1 | 6. Loopback jack |
| 2. Span section 2 | 7. Network interface smart jack |
| 3. Span section 3 | 8. Interface termination or fiber multiplexer (MUX) |
| 4. 120A2 (or later) ICSU | 9. Central office |
| 5. RJ-48 to network interface (up to 1000 ft. [305 m]) | |

Figure 18: Network interface at extended demarcation point (smart jack inaccessible) for a 120A2 (or later) ICSU

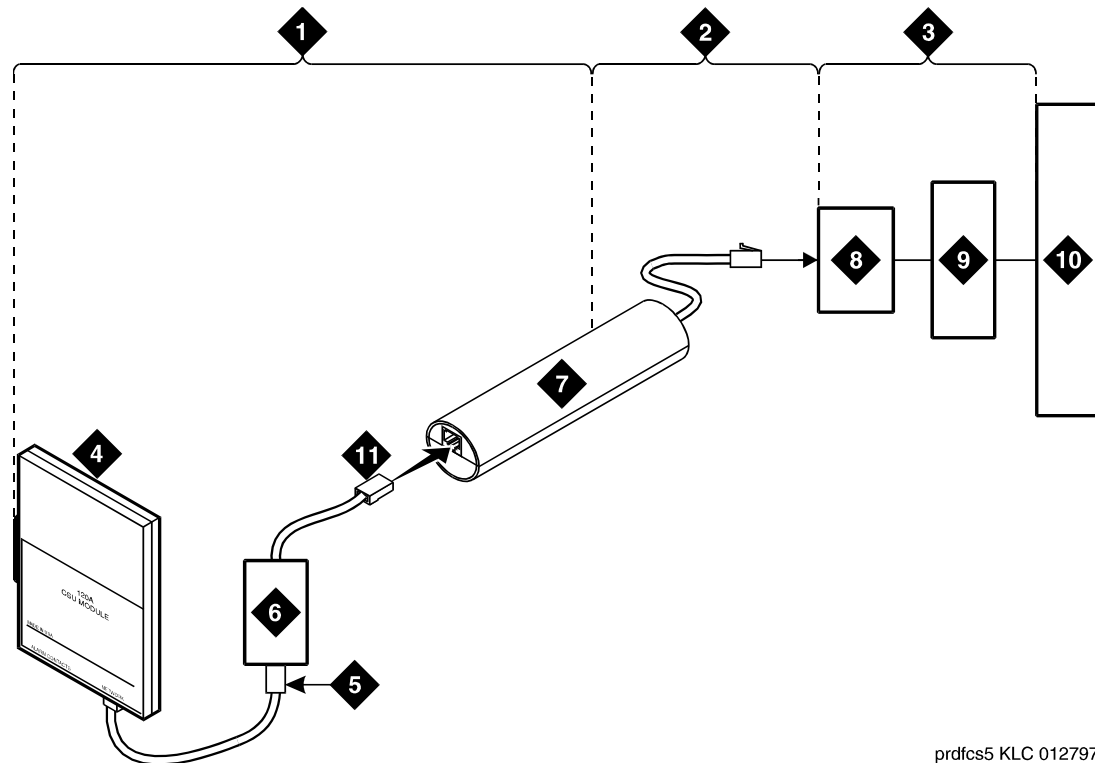


prdfcs4 KLC 012797

Figure notes:

- | | |
|--|---|
| 1. Span section 1 | 6. Loopback jack |
| 2. Span section 2 | 7. Dumb block (extended demarcation) |
| 3. Span section 3 | 8. Network interface smart jack |
| 4. 120A2 (or later) ICSU | 9. Interface termination or fiber multiplexer (MUX) |
| 5. RJ-48 to network interface (up to 1000 ft. [305 m]) | 10. Central office |

Figure 19: Network interface at extended demarcation point (smart jack accessible) for a 120A2 (or later) ICSU



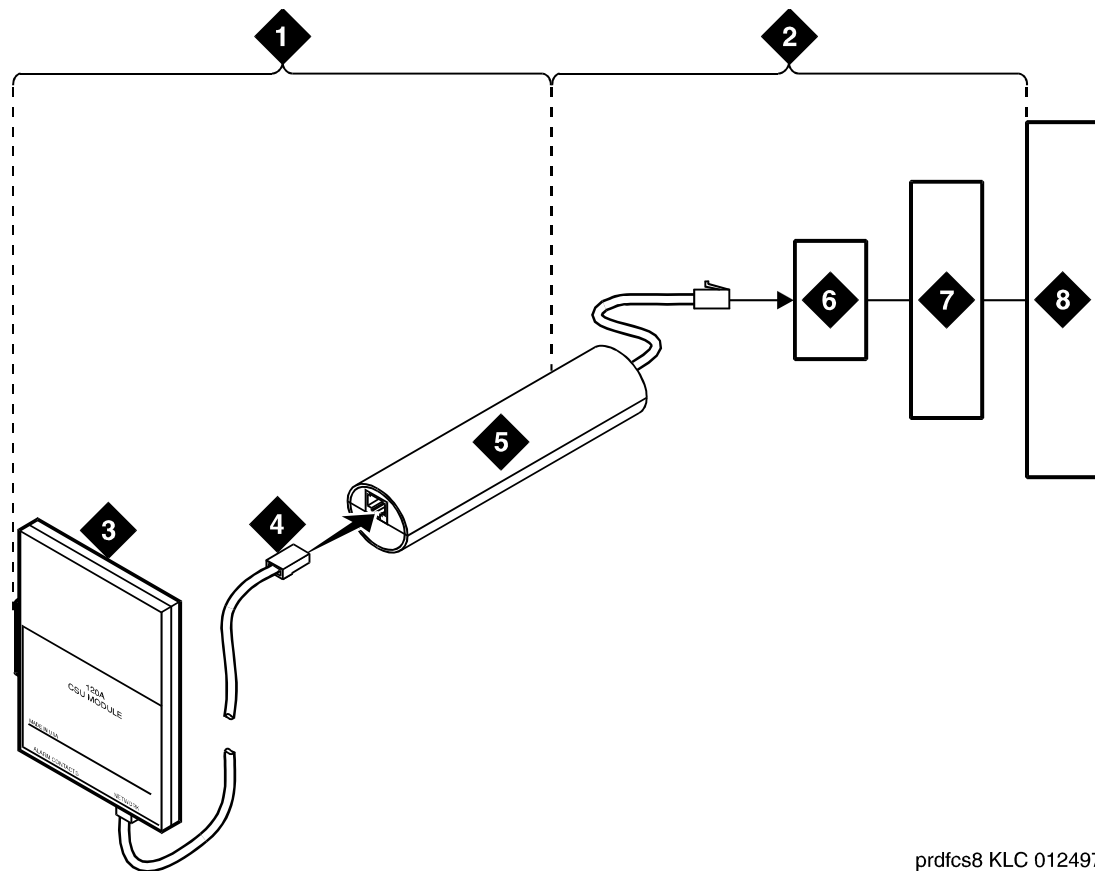
prdfcs5 KLC 012797

Figure notes:

- | | |
|--|---|
| 1. Span section 1 | 6. Dumb block (extended demarcation) |
| 2. Span section 2 | 7. Loopback jack |
| 3. Span section 3 | 8. Network interface smart jack |
| 4. 120A2 (or later) ICSU | 9. Interface termination or fiber multiplexer (MUX) |
| 5. RJ-48 to network interface up to 1000 ft. (305 m) | 10. Central office |
| | 11. Dumb block to smart jack RJ-48 |

Testing a loopback jack without a smart jack

When you add the loopback jack to a span that does not contain a smart jack, the span is divided into 2 sections: from the ICSU or MM710 to the loopback jack and from the loopback jack to the CO. The second section includes the short cable from the loopback jack to the dumb block demarcation point which is a part of the loopback jack. This cable is the only part of Section 2 that is part of customer premises wiring and not covered in the loopback path of the loopback jack. For more information, see [Figure 20: Network interface at “dumb” block for a 120A2 \(or later\) ICSU](#) on page 107 through [Figure 21: Network interface at “dumb” block with repeater line to fiber MUX for a 120A2 \(or later\) ICSU](#) on page 108.

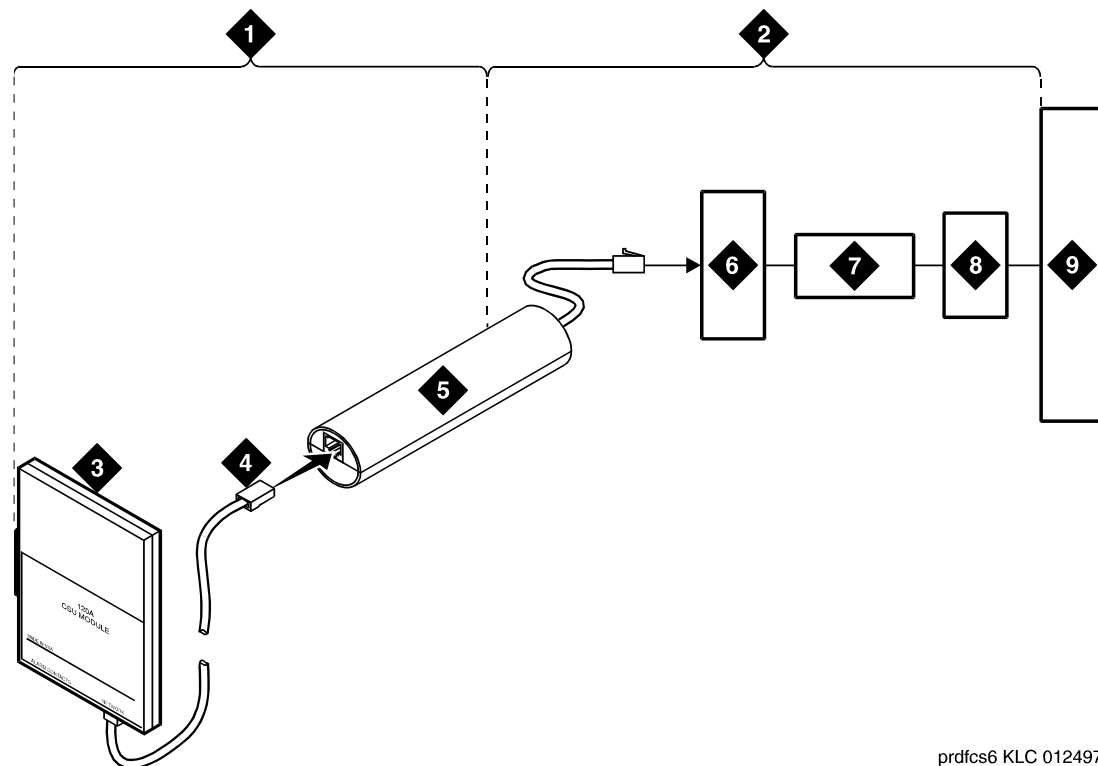
Figure 20: Network interface at “dumb” block for a 120A2 (or later) ICSU

prdfcs8 KLC 012497

Figure notes:

- | | |
|--|---|
| 1. Span section 1 | 5. Loopback jack |
| 2. Span section 2 | 6. Dumb block (demarcation point) |
| 3. 120A2 (or later) ICSU | 7. Interface termination or fiber multiplexer (MUX) |
| 4. RJ-48 to network interface (up to 1000 ft. [305 m]) | 8. Central office |

Figure 21: Network interface at “dumb” block with repeater line to fiber MUX for a 120A2 (or later) ICSU



prdfcs6 KLC 012497

Figure notes:

- | | |
|--|-----------------------------------|
| 1. Span section 1 | 5. Loopback jack |
| 2. Span section 2 | 6. Dumb block (demarcation point) |
| 3. 120A2 (or later) ICSU | 7. Repeater |
| 4. RJ-48 to network interface (up to 1000 ft. [305 m]) | 8. Fiber multiplexer (MUX) |
| | 9. Central office |

You must find and correct the problems in the customer wiring in section 1 and the loopback cable portion of section 2. The DS1 service provider finds and corrects the problems in the majority of section 2.

1. Test customer premises wiring from the ICSU to the loopback jack, as described in the *DS1 Span Test* section.
2. Test the loopback jack-to-*dumb* block and *dumb* block-to-CO wiring. For more information, see section 2 in [Figure 20: Network interface at “dumb” block for a 120A2 \(or later\) ICSU](#) on page 107 through [Figure 21: Network interface at “dumb” block with repeater line to fiber MUX for a 120A2 \(or later\) ICSU](#) on page 108. You can perform this test using one of the following loopbacks that overlap the section of the span:
 - The line loopback of the local ICSU. The DS1 service provider at the CO end typically activates, tests, and then deactivates this loopback.

- The payload loopback of the local DS1 interface. The DS1 service provider at the CO end activates and tests this loopback.
- The line loopback of the far-end ICSU or MM710. To activate this test at the management terminal, type `test ds1-loop location far-csu-loopback-test-begin`, where **location** is the DS1 interface circuit pack corresponding to the loopback jack. To terminate this test, type `test ds1-loop location end-loopback/span-test`, where **location** is the DS1 interface circuit pack corresponding to the loopback jack.

You can examine the bit error counts using the *DS1 Span Test* section. This test only isolates problems in the 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.

Failure in any of the previous tests indicates a problem in Section 2. This problem could be bad loopback jack -to-dumb block cabling. However, the problem can also lie somewhere between the *dumb* block and the CO. The DS1 service provider must address this problem.

If the DS1 Span Test confirms that there are no problems in Section 1, 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 or MM710 line loopback test failed, inform the DS1 provider.
- Request that the DS1 provider perform a loopback test of their portion of the Section 2 wiring. The DS1 provider must send someone out to loop Section 2 back to the CO at the *dumb* block.

If the test fails, the problem is in the service provider wiring.

If the test passes, the problem is in the cable between the loopback jack and the *dumb* block. Replace the loopback jack.

Configurations using fiber multiplexers

Use the loopback jack when the customer premises DS1 wiring connects to an onsite fiber multiplexer (MUX). You can also use the loopback jack if you can perform remote tests of the wiring to the network interface point on the MUX. Set the MM710 CSU to use on DS1 wiring to the MUX.

Fiber MUXs can replace Interface termination feeds. See [Figure 17: Network interface at smart jack for a 120A2 \(or later\) ICSU](#) on page 104 through [Figure 20: Network interface at “dumb” block for a 120A2 \(or later\) ICSU](#) on page 107. Test these spans with the same procedures as metallic spans. Note the following points:

1. Fiber MUXs might have loopback capabilities that the service provider can activate from the CO end. These capabilities might loop the signal back to the CO or back to the DS1 circuit

pack or MM710. If the MUX provides the equivalent of a line loopback on the problem DS1 facility, activate the MUX after a successful loopback jack test. Then use the MUX to isolate problems to the wiring between the loopback jack and the MUX.

2. Some installations use repeater metallic lines between the MUX and the *dumb* block. These lines require DC power for the repeaters and this DC power is present at the *dumb* block interface to the CPE equipment. You need a loopback jack for this configuration to properly isolate and terminate the DC power.

To check the presence of DC, take the following measurements at the network interface jack:

1. From transmit tip (T, Pin 5) to receive tip (T1, Pin 2)
2. From transmit ring (R, Pin 4) to receive ring (R1, Pin 1)
3. From transmit tip (T, Pin 5) to transmit ring (R, Pin 4)
4. From receive tip (T1, Pin 2) to receive ring (R1, Pin 1)

All measurements should read zero (0) volts DC. For more information about pin numbers and pin designations, see *Integrated CSU Module Installation and Operation*, 555-230-193.

ISDN converters and adapters

ISDN converters and adapters are sometimes necessary when you connect to coaxial facilities in a multicarrier cabinet or a single-carrier cabinet.

Connections include:

- Integrated Services Data Network Primary Rate Interface (ISDN-PRI) to Direct Access Secondary Storage (DASS)
- PRI to Digital Private Network Signaling System (DPNSS)
- PRI to ISDN Basic Rate Interface (ISDN-BRI)

Converter circuit packs are known as common channel signaling converter (CCSC), types 1 and 2.

Converters for single-carrier cabinets

PRI-to-DASS and PRI-to-DPNSS converters

[Figure 22: Typical DASS or DPNSS converter cable connections](#) shows typical connections from the CCSC-1 PRI-to-DASS converter or the CCSC-2 PRI-to-DPNSS converters to the coaxial facility.

Figure 22: Typical DASS or DPNSS converter cable connections

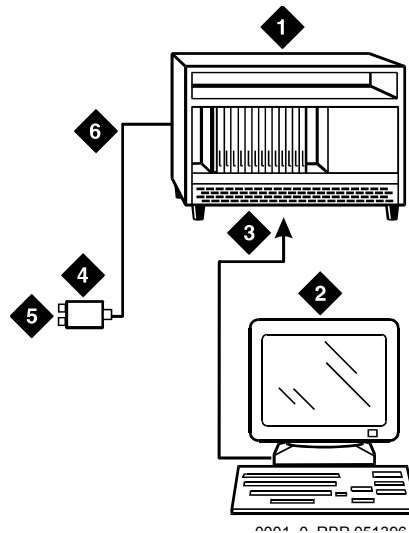


Figure notes:

- | | |
|---|---|
| 1. To TN464F DS1 circuit pack and either a CSCC-1 PRI-to-DASS converter or a CSCC-2 PRI-to-DPNSS converter circuit pack | 4. 888B coaxial converter |
| 2. Communication Manager administration PC | 5. Coaxial connection to 2-Mbps facility |
| 3. RS-232 cable to front of PRI converter circuit pack | 6. Coaxial cable from PRI converter circuit pack to coaxial converter |

1. Plug the PC into the RS-232 connector on the front of the PRI converter circuit pack.
2. Connect the coaxial Y-cable from the TN464F to the PRI converter circuit pack.
3. Connect the opposite end of the Y-cable to the 888B coaxial converter.

PRI-to-BRI converter

[Figure 23: Typical PRI to BRI converter cable connections](#) shows typical connections from the PRI-to-BRI converter to the coaxial facility.

Figure 23: Typical PRI to BRI converter cable connections

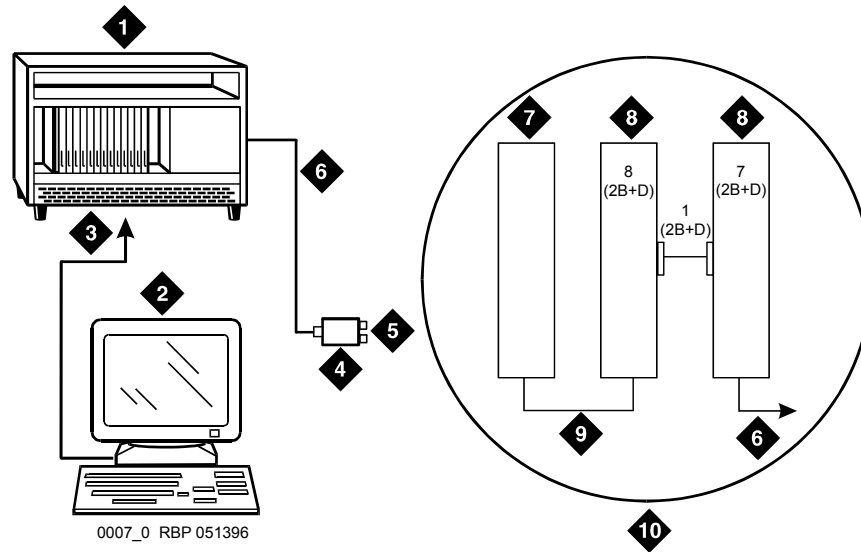


Figure notes:

- | | |
|--|--|
| <ul style="list-style-type: none"> 1. To TN464F DS1 circuit pack and PRI-to-BRI converter circuit pack 2. Communication Manager administration PC 3. RS-232 cable to the front of the converter circuit pack 4. 888B coaxial converter 5. Coaxial connection to 2-Mbps facility | <ul style="list-style-type: none"> 6. Coaxial cable from PRI converter circuit pack to coaxial converter 7. TN464F circuit pack 8. PRI-to-BRI converter circuit pack 9. Jumper coaxial cable 10. Inset showing connections on the rear of the carrier |
|--|--|

Note:

The inset shows details of the cable connections between the circuit packs. Connect the Communication Manager administration PC to the RS-232 connector on the front of the PRI converter circuit pack.

Converters for multicarrier cabinets

PRI-to-DASS and PRI-to-DPNSS converters

The following steps connect the administration PC to the PRI converter.

- Connect the Communication Manager administration PC to the RS-232 connector on the front of the PRI converter circuit pack.

[Figure 24: Typical DASS or DPNSS converter cable connections](#) shows typical connections from the CCSC-1 PRI-to-DASS converter or the CCSC-2 PRI-to-DPNSS converters to the coaxial facility.

Figure 24: Typical DASS or DPNSS converter cable connections

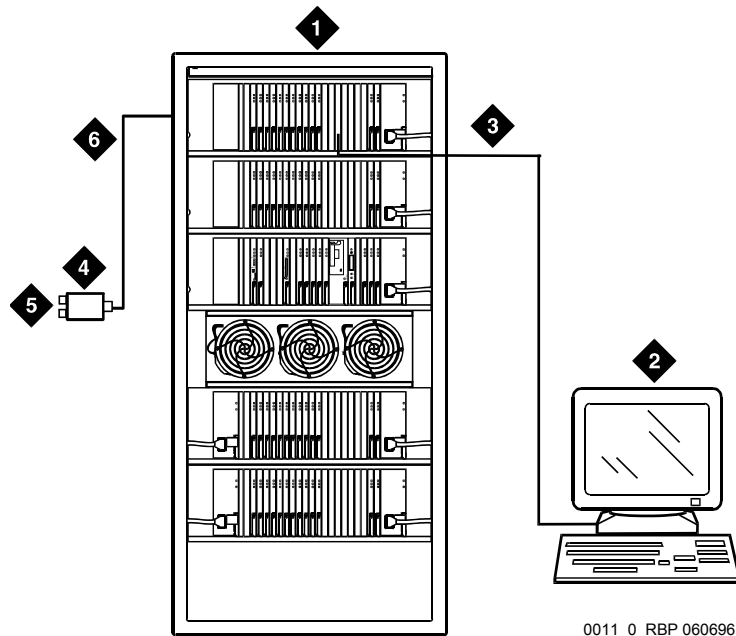


Figure notes:

- | | |
|---|---|
| 1. To TN464F DS1 circuit pack and either a CSCC-1 PRI-to-DASS converter or a CSCC-2 PRI-to-DPNSS converter circuit pack | 4. 888B coaxial converter |
| 2. Communication Manager administration PC | 5. Coaxial connection to 2-Mbps facility |
| 3. RS-232 cable to front of PRI converter circuit pack | 6. Coaxial cable from PRI converter circuit pack to coaxial converter |

PRI-to-BRI converter

[Figure 25: Typical PRI to BRI converter cable connections](#) shows typical connections from the PRI-to-BRI converter to the coaxial facility. The Communication Manager administration PC is connected to the RS-232 connector on the front of the PRI converter circuit pack.

Figure 25: Typical PRI to BRI converter cable connections

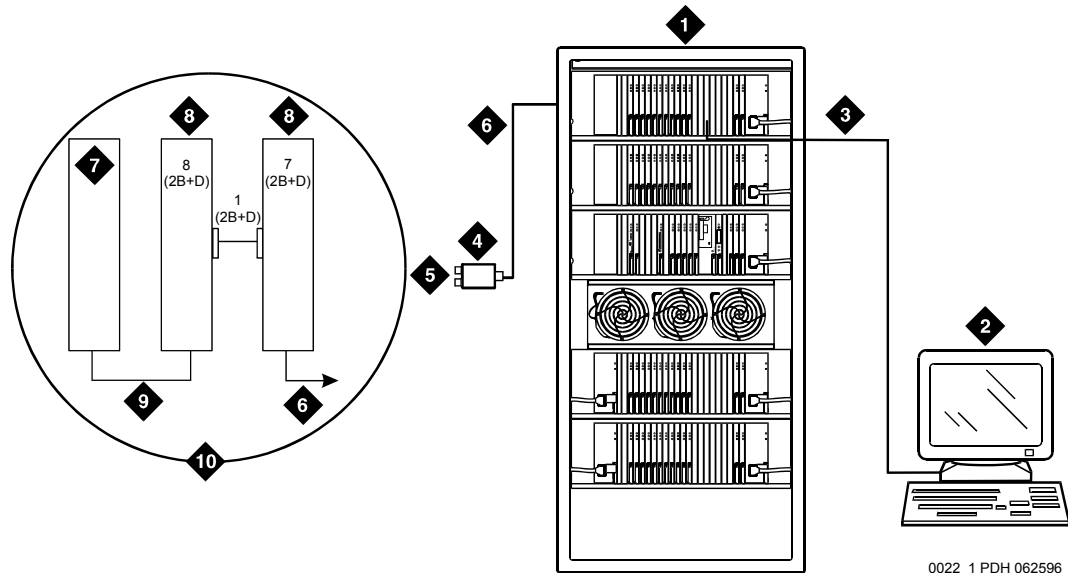


Figure notes:

- | | |
|---|---|
| 1. TN464F DS1 circuit pack and PR-to-BRI converter circuit pack | 6. Coaxial cable from PRI converter circuit pack to coaxial converter |
| 2. Communication Manager administration PC | 7. TN464F circuit pack |
| 3. RS-232 cable to the front of the converter circuit pack | 8. PRI-to-BRI converter circuit pack |
| 4. 888B 75-ohm coaxial converter | 9. Jumper coaxial cable |
| 5. Coaxial connection to 2-Mbps facility | 10. Inset showing connections on the rear of the carrier |

Note:

The inset shows details of the cable connections between the circuit packs.

Busy tone disconnect equipment for non-U.S. installations

The customer-provided busy tone disconnect adjunct detects busy tone disconnects of incoming calls on loop-start, 2-wire, analog trunks. In some non-U.S. countries where a G700 or

G350 Branch Gateway is used, the PSTN sends busy tone as the disconnect signal. Therefore, the S8300D Server, G700 Branch Gateway, or G350 Branch Gateway requires a busy tone disconnect adjunct. [Figure 26: Typical cabling for busy tone disconnect](#) on page 115 shows typical connections.

Figure 26: Typical cabling for busy tone disconnect

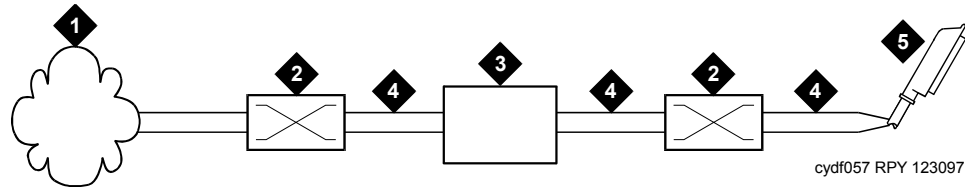


Figure notes:

- | | |
|--------------------------------------|---|
| 1. Public switched telephone network | 4. Tip and ring wires |
| 2. Main distribution frame | 5. To loop-start, central-office, trunk |
| 3. Busy tone disconnect device | MM711 analog media module |

909A/B universal coupler

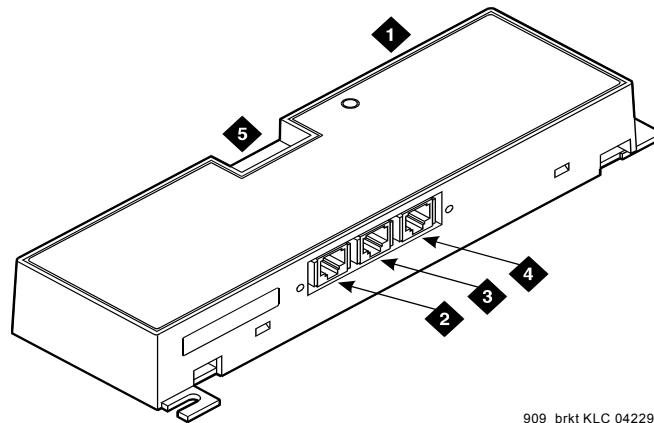
The 909A/B universal coupler is used with paging, malicious call trace, and music-on-hold equipment that is not approved for use with the public network.

[Figure 27: Typical 909A/B universal coupler](#) on page 116 shows a typical 909A/B universal coupler. For additional installation and switch setting information, see *909A/909B Universal Coupler Installation Instructions*, which is usually shipped with the 909A/909B Universal Coupler.

Note:

If the music source is registered by the FCC in the USA or an equivalent body, you do not require the 909A/B universal coupler.

Figure 27: Typical 909A/B universal coupler



909 brkt KLC 042296

Figure notes:

- | | |
|-----------------------------|--------------------------|
| 1. 909A/B universal coupler | 4. J3 7-pin modular jack |
| 2. J1 8-pin modular jack | 5. DIP switch location |
| 3. J2 8-pin modular jack | |

The 909A is the direct current (DC) version of the coupler, and cabinet power supplies -48 VDC power. The 909B is the alternating current (AC) version, and power is supplied from a separate power supply such as the KS-22911L2.

The DIP switches on the unit set:

- Protection/Paging selection: For AUX trunk paging and malicious call trace, set to C2. For all other applications, set the switch to C1.
- Output attenuation (-9 or -15 dBm): The setting depends on the output level of the music source.
- Output impedance (8 ohms, 1.5 k Ω , and 50 k Ω). Set this switch only if the Protection/Paging switch is set to C2 and the coupler is supplying background music to a customer-supplied paging amplifier.

For the pinouts for J1, J2, and J3, see [Table 10: J1 Pin Assignments \(System Connections\)](#) on page 117, [Table 11: J2 Pin Assignments \(Accessory Connections\)](#) on page 117, and

[Table 12: J3 Pin Assignments \(Power Connections\)](#) on page 118. Use these tables when connecting music or paging equipment.

Table 10: J1 Pin Assignments (System Connections)

Pin	Color	Designation	Description
1	White-Orange	—	Not used
2	Orange	PG2/BZ2	Seizure control lead, connected to -48 VDC from the system or from the 909A/B when the protection paging switch is set to C2, or to -48 VDC on the 909A/B when protection/paging switch is set to C1
3	White-Green	PG1/BZ1	Seizure control lead, connected to SZ lead from the AUX trunk when the protection/paging switch is set to C2, or to -48 VDC on the 909A/B when the protection/paging switch is set to C1
4	Blue	R	Ring lead
5	White-Blue	T	Tip lead
7	Green	BSY2/BY2	Busy/busy-out lead, connected to S1 lead from the AUX trunk
7	White-Brown	BSY1/BY1	Busy/busy-out lead, connected to S lead from the AUX trunk
8	Brown	—	Not Used

Table 11: J2 Pin Assignments (Accessory Connections)

Pin	Color	Designation	Description
1	White-Orange	CMS1/M1	Customer-supplied music source
2	Orange	CMS2/M2	Customer-supplied music source
3	White-Green	COS1	Remote busyout control contact closure from music source
4	Blue	CR	Customer ring lead
5	White-Blue	CT	Customer tip lead
7	Green	COS2	Remote busyout control contact closure from music source
7	White-Brown	CBS1/C1	Seizure indication provided to music source
8	Brown	CBS2/C2	Seizure indication provided to music source

CAUTION:
To prevent damage to the 909A/B universal coupler, do not plug the cable into J3 before all cross-connects are complete.

Table 12: J3 Pin Assignments (Power Connections)

Pin	Color	Designation	Description
1, 3, 4, & 7	—	—	Not used
2	Black	GRD	-48 RET or ground lead from system or from positive lead of power supply
5	Yellow	-48 VDC	-48 VDC from system or from negative lead of power supply

Figure 28: [Typical modular jack pinout](#) shows the physical locations of the pins for J1, J2, and J3.

Figure 28: Typical modular jack pinout

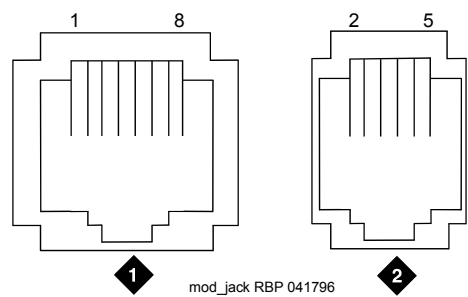


Figure notes:

1. J1 and J2 8-pin modular jacks
2. J3 7-pin modular jack

Malicious call trace

The malicious call trace (MCT) voice recorder connects directly to the tip and ring connections of a TN763/D auxiliary trunk circuit pack. See [Figure 29: Malicious call trace](#). The 909A/B universal coupler provides seizure control to the recorder.

Note:

G700 or G350 Branch Gateway does not include an auxiliary trunk circuit pack. Therefore, information in this chapter is not relevant to these branch gateways. But you can use the information to gain access to the MCT equipment connected to a port network.

Figure 29: Malicious call trace

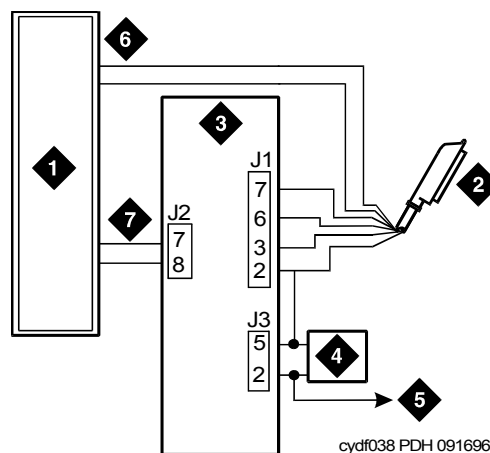


Figure notes:

- | | |
|---|---------------------------------------|
| 1. Malicious call trace voice recorder | 4. Power supply for universal coupler |
| 2. 25-pair cable (T, R, S, S1, Sz, SZ1) to TN763/D auxiliary trunk circuit pack | 5. To SZ1 on TN763/D connector |
| 3. 909A/B universal coupler | 6. Tip and ring wires |
| | 7. CBS1/C1 and CBS2/C2 |

Note:

A wiring block must be locally engineered.

Note:

909A couplers ship with one DW4B-DE cable and two DW8B-SE cables. The 909B ships with one KS-22911L2 power supply, one DW4B-DE cable, and two DW8B-SE cables.

1. Determine the port assignment of the recorder from the malicious call tracing form.
2. Install the 909A/B universal coupler on a vertical surface.
3. Connect the SZ, SZ1, S, and S1 leads from the 909A/B to an auxiliary trunk circuit pack.

Adjuncts and peripherals

- a. Tip and ring connect from the voice recorder to the auxiliary trunk circuit pack J1 on the 909A/B.
- b. CBS1/C1 and CBS2/C2 connect from the voice recorder to J2 on the 909A/B.
4. On the 909A/B universal coupler:
 - a. Connect seizure control voltage of -9 to -70 Volts to the PG2/BZ2 connection (pin 2 of J1). Switching voltage to the PG2/BZ2 connection can be from the 909A/B -48 VDC supply.
 - b. Connect SZ1 to the ground lead of the DC power source used for PG2/BZ2.
 - c. Set S1 to the "C2" position. Set S2 position 7 to "OPEN".
 - d. Connect an approved -48 VDC power source to the **-48** and **GRD** terminals (pins 5 and 2, respectively, of J3 on the 909A/B).
5. Administer the switch for the call trace device.

Note:

For more information about installation, see *909A/909B Universal Coupler Installation Instructions*, which is usually shipped with the 909A/909B Universal Coupler.

Music-on-hold

With the music-on-hold (MOH) feature, a caller hears music when that caller is placed on hold.

To provide music-on-hold, use a two-wire TN2183 analog line circuit pack or equivalent or an auxiliary trunk circuit pack to a customer-supplied music source.

Music-on-hold is available on the following gateways:

- G650 Media Gateway
- G700 Branch Gateway: Through a port on an MM711 Analog Media Module to a customer-supplied music source on a G700 Branch Gateway.
- G350 Branch Gateway: Through a port on an MM711 Analog Media Module or MM714 Analog Media Module or through a fixed analog port (LINE 1 or LINE 2) to a customer-supplied music source on a G350 Branch Gateway.

[Figure 30: Typical registered equipment connections \(auxiliary access\) for G650 Branch Gateway](#) on page 121 shows the connections for music-on-hold, dial dictation, or recorded announcement features when the music source is Federal Communications Commission (FCC) registered (or equivalent). [Figure 31: Typical nonregistered equipment connections \(auxiliary access\) for G650 Branch Gateway](#) on page 122 shows the connections when the music source is not FCC-registered or equivalent.

Local music-on-hold allows one music source. However, if you purchase the multiple music-on-hold (tenant partitioning) feature, you can have up to 100 music sources.

Note:

Use the following connection instructions when the music source is not located in the equipment room. If the music source is located in the equipment room, do not route the connections through the information outlet.

Figure 30: Typical registered equipment connections (auxiliary access) for G650 Branch Gateway

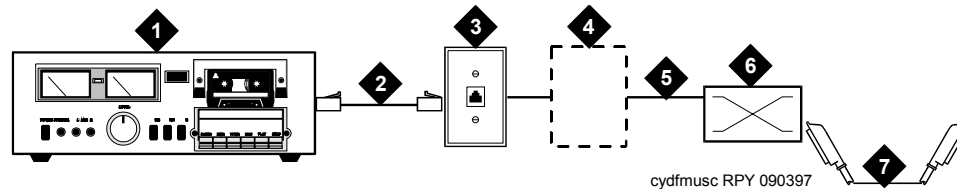


Figure notes:

- | | |
|--|--|
| 1. Music source | 5. Tip (green) and ring (red) |
| 2. 4-pair modular cord | 6. Part of main distribution frame |
| 3. 103A or modular wall jack | 7. A25D 25 pair cable (male-to-male) to auxiliary trunk circuit pack |
| 4. 122A music adapter (if required—primarily required in France) | |

-
1. If the music source is registered, the system side of the MDF connects directly to the system.
 2. If the music source is not registered, the system side of the MDF connects to a 909A/B universal coupler (see [909A/B universal coupler](#) on page 115).

Registered music source

See [Figure 30: Typical registered equipment connections \(auxiliary access\) for G650 Branch Gateway](#) on page 121 to install a registered music source.

1. Determine feature port assignment from the Feature-Related System Parameters screen.
2. Install the music source according to the manufacturer instructions.
3. Install patch cord/jumper wires at the main distribution frame.
4. Administer the switch for the new equipment.

Nonregistered music source

See [Figure 31: Typical nonregistered equipment connections \(auxiliary access\) for G650 Branch Gateway](#) on page 122 and [Figure 32: Connections to nonregistered music-on-hold](#)

[using analog line for G650 Branch Gateway](#) on page 123 when installing a nonregistered music source.

1. Determine feature port assignment from Feature-Related System Parameters Form.
2. Install the music source according to the manufacturer instructions.
3. Connect a cable from the assigned port carrier slot to J1 on the 909A/B universal coupler. For more information, see [909A/B universal coupler](#) on page 115. A wiring block must be locally engineered.
 - a. Connect the T-lead at pin 5 and the R-lead at pin 4 of J1 on the 909A/B universal coupler to the corresponding leads from the TN2183.
 - b. Connect the CT-lead at pin 5 and the CR-lead at pin 4 of J2 on the 909A/B universal coupler to the MDF.
4. Install patch cord/jumper wires at the MDF to connect tip and ring to the information outlet at the music source.
5. Set the Protection/Paging switch to C1.
6. Connect a modular cord from the information outlet to the music source.
7. Connect -48V to pin 5 and -48V RET to pin 2 of J3 on the 909A/B. The power source can be an 1151A, 1151A2, or other approved power supply.
8. Administer the switch for the new equipment.

Figure 31: Typical nonregistered equipment connections (auxiliary access) for G650 Branch Gateway

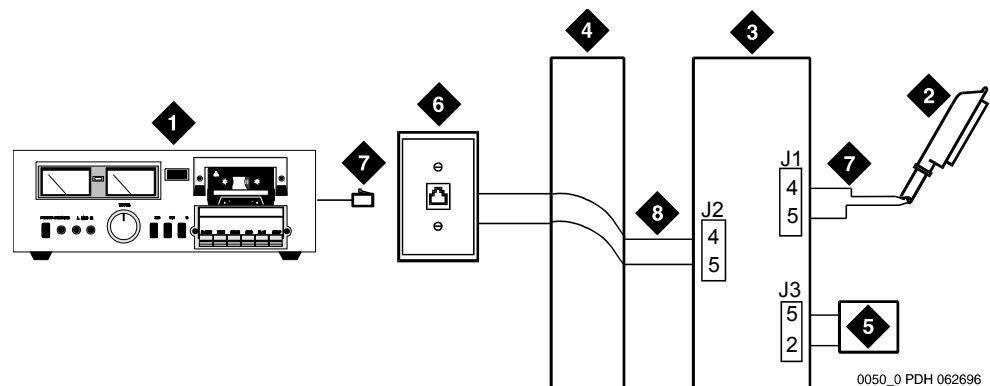


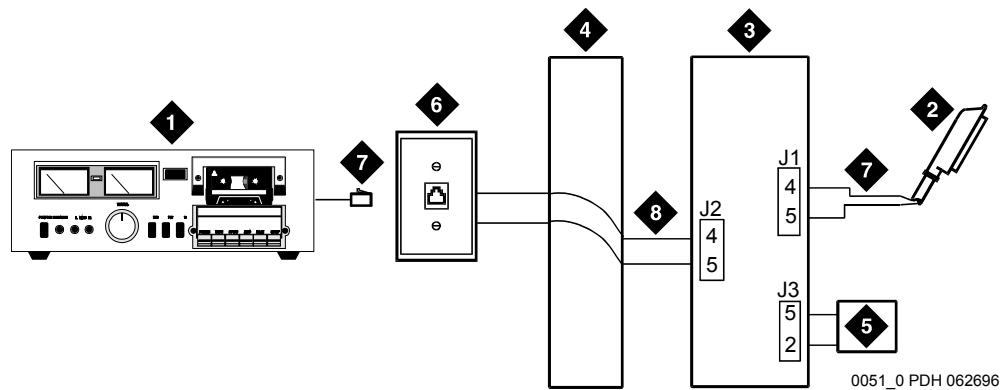
Figure notes:

- | | |
|---|---------------------------------------|
| 1. Customer-supplied music source | 5. Power supply for universal coupler |
| 2. A25D 25-pair cable to auxiliary trunk circuit pack | 6. 103A or modular wall jack |
| 3. 909A/B universal coupler | 7. 4-pair modular cord |
| 4. Part of main distribution frame | 8. Tip and ring wires |

Note:

A wiring block must be locally engineered.

Figure 32: Connections to nonregistered music-on-hold using analog line for G650 Branch Gateway

**Figure notes:**

- | | |
|--|---------------------------------------|
| 1. Customer-supplied music source | 5. Power supply for universal coupler |
| 2. 25-pair cable to analog line circuit pack | 6. 103A or modular wall jack |
| 3. 909A/B universal coupler | 7. 4-pair modular cord |
| 4. Part of main distribution frame | 8. Tip and ring wires |

Note:

A wiring block must be locally engineered.

Note:

For more information about installation, see *909A/909B Universal Coupler Installation Instructions*, which is usually shipped with the 909A/909B Universal Coupler.

On a G700 or G350 Branch Gateway, the music-on-hold feature is connected through a port on an MM711 Analog Media Module or, for a G350 Branch Gateway only, an MM714 Analog Media Module or the analog LINE ports of the integrated analog media module.

The G700 or G350 Branch Gateway does not support an auxiliary trunk circuit pack. Therefore, these branch gateways do not support the music-on-hold feature through an auxiliary trunk for S8300D Server users. However, G700 or G350 Branch Gateway users with an S8510 or S8800 Server as primary controller can access the music-on-hold feature if their equipment is physically connected to a TN763 auxiliary trunk circuit pack in an EPN carrier of an S8510 or S8800 system.

Unregistered music source on a G700 or G350 Branch Gateway

[Figure 33: Unregistered music-on-hold equipment connecting to KS-23395-L3 for a G700 Branch Gateway](#) on page 124 and [Figure 34: Unregistered music-on-hold equipment](#)

[connecting to KS-23395-L4 for a G700 Branch Gateway](#) on page 125 show the connections for the music-on-hold feature on a G700 Branch Gateway for an unregistered source.

Note:

The G350 Branch Gateways physical connection with the MM711 Analog Media Module, MM714 Analog Media Module, or fixed analog ports (LINE 1 or 2) on the front panel is the same as the G700 Branch Gateways connection with the MM711 Analog Media Module.

Note:

If you want multiple music sources, you must use multiple ports on the MM711 Analog Media Module.

Figure 33: Unregistered music-on-hold equipment connecting to KS-23395-L3 for a G700 Branch Gateway

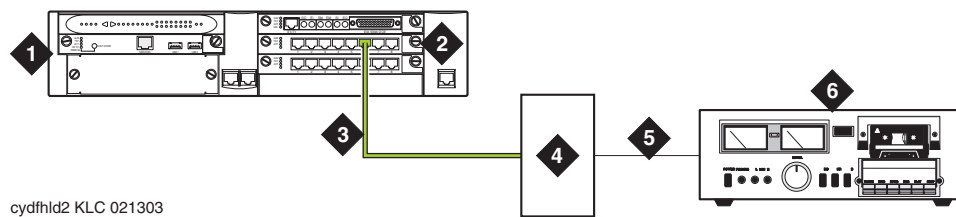


Figure notes:

- | | |
|------------------------------|------------------------|
| 1. G700 Branch Gateway | 4. KS-23395-L3 coupler |
| 2. MM711 Analog Media Module | 5. RCA cord |
| 3. RJ-45 connection | 6. Music source |

To hook up an unregistered music-on-hold source to a G700 or G350 Branch Gateway using a KS-23395-L3 coupler:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module. Or, for a G350 Branch Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the other end of the RJ-45 cable to a KS-23395-L3 coupler.
3. Connect the KS-23395-L3 coupler to the customer-supplied music source. Follow the manufacturers instructions to properly connect the music source to the KS-23395-L3 coupler. Normally, you simply use an RCA cord.
4. Administer the switch for the new equipment.

Figure 34: Unregistered music-on-hold equipment connecting to KS-23395-L4 for a G700 Branch Gateway

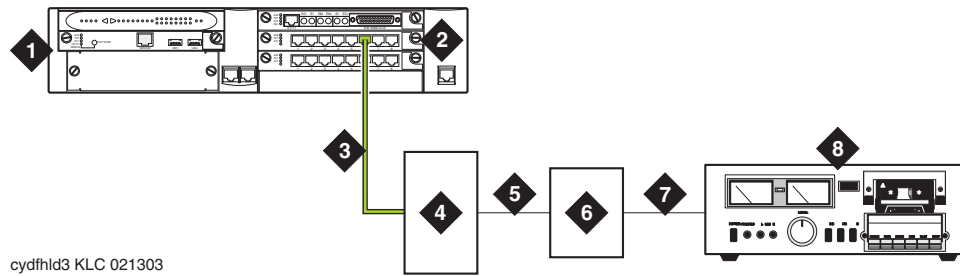


Figure notes:

- | | |
|------------------------------|-----------------------------|
| 1. G700 Branch Gateway | 5. 8-pair modular cord |
| 2. MM711 Analog Media Module | 6. 909A/B universal coupler |
| 3. RJ-45 connection | 7. 8-pair modular cord |
| 4. KS-23395-L4 coupler | 8. Music source |

To hook up an unregistered music-on-hold source to a G700 or G350 Branch Gateway using a KS-23395-L4 coupler:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module. Or, for a G350 Branch Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the other end of the RJ-45 cable to a KS-23395-L4 coupler.
3. Connect the KS-23395-L4 coupler to the 909A/B universal coupler using an 8-pair modular cord.
4. Connect the 909A/B universal coupler to the music source using an 8-pair modular cord.
5. Administer the switch for the new equipment.

Note:

For additional installation information, see *909A/909B Universal Coupler Installation Instructions*, which is normally shipped with the 909A/909B Universal Coupler.

Registered music source on a G700 or G350 Branch Gateway

[Figure 35: Registered music-on-hold equipment connecting to KS-23395-L4 for a G700 Branch Gateway](#) on page 126 shows the connections for the music-on-hold feature on a G700 Branch Gateway for an unregistered source.

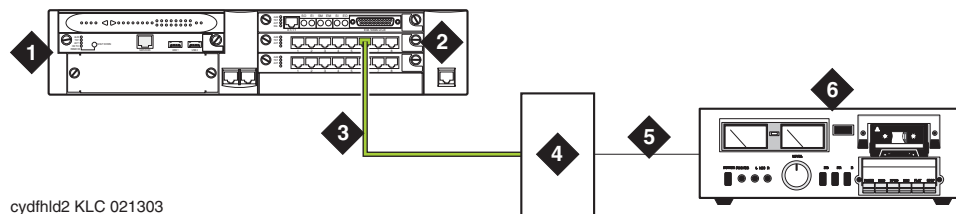
Note:

The G350 Branch Gateway's physical connection with the MM711 Analog Media Module, MM714 Analog Media Module, or fixed analog ports (LINE 1 or 2) on the front panel is the same as the G700 Branch Gateway's connection with the MM711 Analog Media Module.

Note:

If you want multiple music sources, you must use multiple ports on the MM711 Analog Media Module.

Figure 35: Registered music-on-hold equipment connecting to KS-23395-L4 for a G700 Branch Gateway

**Figure notes:**

- | | |
|------------------------------|------------------------|
| 1. G700 Branch Gateway | 4. KS-23395-L4 coupler |
| 2. MM711 Analog Media Module | 5. 8-pair modular cord |
| 3. RJ-45 connection | 6. Music source |

To hook up an registered music-on-hold source to a G700 or G350 Branch Gateway using a KS-23395-L4 coupler:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module. Or, for a G350 Branch Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the KS-23395-L4 coupler to the customer-supplied music source. Normally, you simply use a 8-pair modular cord.
3. Administer the switch for the new equipment.

Paging and announcement equipment

This section explains the most common system configurations for the paging feature of Communication Manager. This chapter provides information on the following features:

- [Loudspeaker paging](#)
- [ESPA radio paging](#)

- [External ringing](#)
- [Queue warning indicator](#)
- [Loudspeaker paging](#)

Loudspeaker paging

In a G650 Gateway, the loudspeaker paging feature provides a connection from a TN763B/C/D auxiliary trunk circuit pack (or equivalent) to a customer-supplied paging amplifier.

Loudspeaker paging without paging adapter

[Figure 36: Connections for loudspeaker paging without paging adapter for G650 Branch Gateway](#) on page 128 shows the connections for the loudspeaker paging feature. These connections are used when the loudspeaker interface equipment is not located in the equipment room. If the equipment is located in the equipment room, the information outlet is not required. The connections shown are for one zone.

[Figure 36: Connections for loudspeaker paging without paging adapter for G650 Branch Gateway](#) on page 128 also shows connections from an optional customer-supplied music source to the loudspeaker system through a paging amplifier, as well as connections to the loudspeaker system through a 909A/B universal coupler (see [909A/B universal coupler](#) on page 115).

Note:

If the loudspeaker paging system provides a talkback microphone at the speakers, the microphone must be FCC approved or equivalent, or a 909A/B universal coupler is required.

Figure 36: Connections for loudspeaker paging without paging adapter for G650 Branch Gateway

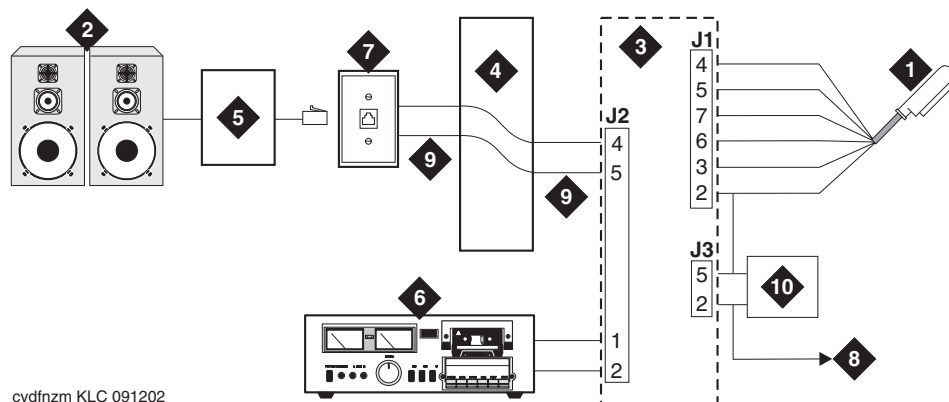


Figure notes:

- | | |
|---|---|
| 1. 25-pair cable to TN763B/C/D auxiliary trunk circuit pack | 6. Music source for background music over loudspeakers (optional) |
| 2. Loudspeaker paging system | 7. 103A or modular wall jack |
| 3. 909A/B universal coupler (if required) | 8. To SZ1 on TN763 connector |
| 4. Part of main distribution frame (MDF) circuits 1-16 | 9. Tip and ring wires |
| 5. Paging amplifier | 10. -48 VDC power supply for 909B |

Note:

On the 25-pair cable to TN763B/C/D auxiliary trunk circuit pack, SZ1 connects to GRD on key 10. The 50 points amphenol is connected to the back of a G600 or G650 Branch Gateway.

Loudspeaker paging access without universal coupler

To install the loudspeaker equipment:

1. Determine the port assignment of paging zones from the Loudspeaker Paging screen.
2. At the main distribution frame, locate the connecting block and terminals assigned to the selected port.
3. On the locally engineered wiring block, place a strap between terminals S and SZ and terminals S1 and SZ1.
4. Install patch cord/jumper wires at the main distribution frame.
5. Connect a 2-pair line cord, with a modular plug at one end, from the information outlet to the paging amplifier of the loudspeaker system.
6. Install loudspeaker equipment according to the manufacturer instructions.
7. Administer the switch for the new equipment.

Loudspeaker paging with universal coupler

An information outlet provides access to loudspeaker paging. The system side of the main distribution frame connects to a 909A/B universal coupler. Make provisions for the **DC** power that the 909A/B universal coupler requires, such as a 1151A, 1151A2, or other approved -48VDC power supply.

Six leads (T, R, SZ, SZ1, S, and S1) connect the adapter to an auxiliary trunk circuit pack located in a port carrier.

1. Determine the port assignment of paging zones from the Loudspeaker Paging screen.
2. Identify the carrier slot and label at both ends of an A25D or male-to-male cable.
3. Connect a cable from the 909A/B to the system side of the main distribution frame. A wiring block must be locally engineered.
4. [909A/B universal coupler](#) on page 115 provides details of the connections between the 909A/B universal coupler and the wiring blocks.



CAUTION:

To prevent damage to the 909A/B universal coupler, do not plug the cable into J3 before all cross-connects are complete

5. On the 909A/B universal coupler:
 - Connect seizure control voltage of -9 to -70 volts to the PG2/BZ2 connection (pin 2 of J1). Switching voltage to the PG2/BZ2 connection can be from the 909-48-volt supply.
 - Connect a -48 VDC power source to the -48 and GRD terminals on the 909A/B.
6. Install patch cord/jumper wires at the main distribution frame.
7. Connect a 2-pair line cord (modular plug at one end) from the information outlet to the loudspeaker system.
8. Install loudspeaker equipment according to the manufacturer instructions.
9. Connect an approved -48 VDC power source to the **-48** and **GRD** terminals (pins 5 and 2, respectively, of J3).
10. Administer the switch for the new equipment.

Note:

For more information about installation, see *909A/909B Universal Coupler Installation Instructions*, which is usually shipped with the 909A/909B Universal Coupler.

ESPA radio paging

[Figure 37: Typical ESPA radio paging connections](#) shows typical connections to European Standard Paging Access (ESPA) equipment. Connect the LINE jack on the PassageWay interface to a digital line 4-wire DCP circuit pack through the MDF.

Figure 37: Typical ESPA radio paging connections

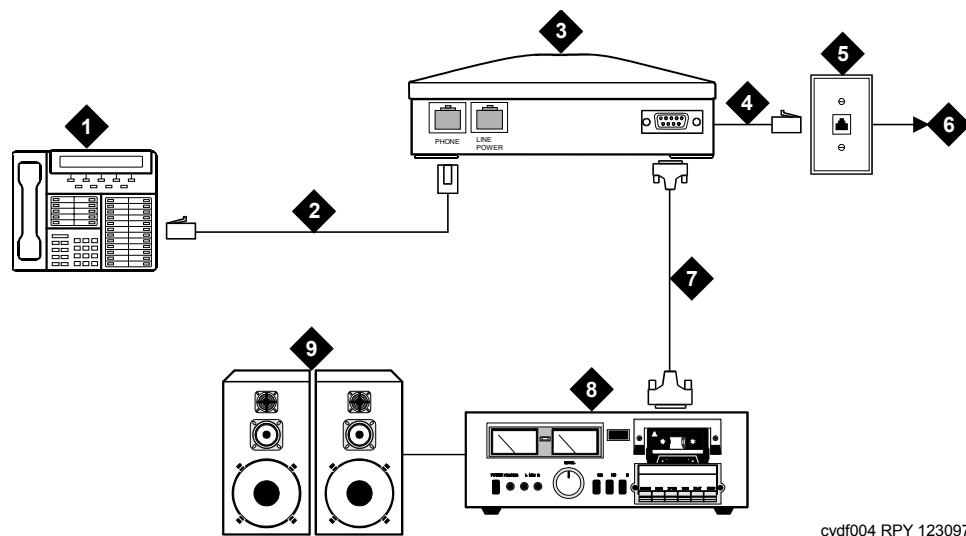


Figure notes:

- | | |
|------------------------------|---------------------------------|
| 1. DCP telephone | 6. To digital line circuit pack |
| 2. 4-pair modular cord | 7. RS-232 connector |
| 3. PassageWay interface | 8. ESPA radio paging equipment |
| 4. 4-pair modular cord | 9. Loudspeaker paging system |
| 5. 103A or modular wall jack | |

External ringing

Connections for external ringing are at an information outlet. The system side of the main distribution frame (MDF) is connected to a TN2183 or equivalent analog line circuit pack in the G650 gateways:

Note:

Up to three devices can be connected to one analog line circuit pack port.

1. Wire the ringing device to the information outlet.
2. Administer the switch for the new equipment.

Queue warning indicator

The connections for the queue warning indicator are the same as external ringing. An AC indicator (light) such as a 21C49 can be used in a Uniform Call Distribution/Direct Departmental Calling (UCD/DDC) queue. The light is connected to an information outlet. The system side of the MDF is connected to an analog line circuit pack located in a port carrier.

1. Wire the queue warning indicator to the information outlet.
2. Administer the switch for the new equipment.

Loudspeaker paging

On a G700 or G350 Branch Gateway, the loudspeaker paging feature is connected through a port on an MM711 Analog Media Module.

The G700 or G350 Branch Gateway does not support an auxiliary trunk circuit pack. Therefore, the loudspeaker feature through an auxiliary trunk is not supported on a G700 or G350 Branch Gateway.

Note:

Users on a G700 or G350 Branch Gateway controlled by an S8800 or S8510 can also access the loudspeaker paging feature if equipment is physically connected to a TN763 auxiliary trunk circuit pack in an PN carrier of an S8800 or S8510 system.

[Figure 38: Typical loudspeaker equipment connections for a G700 or G350 Branch Gateway](#) on page 131 shows the connections for loudspeaker paging, dial dictation, or recorded announcement features on a G700 or G350 Branch Gateway.

Figure 38: Typical loudspeaker equipment connections for a G700 or G350 Branch Gateway

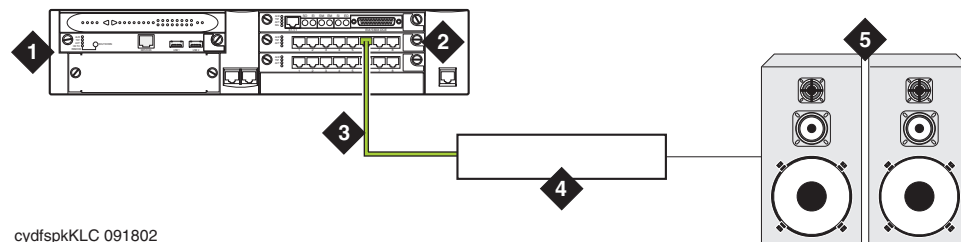


Figure notes:

- | | |
|--------------------------------|--|
| 1. G700 or G350 Branch Gateway | 4. Telephone hybrid (third party) device |
| 2. MM711 Analog Media Module | 5. Loudspeaker paging system |
| 3. RJ-45 connection | |

To hook up loudspeaker paging from a G700 or G350 Branch Gateway:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.
2. Connect the other end of the RJ-45 cable to a customer-supplied telephone hybrid device.
3. Follow the manufacturer's instructions to properly connect the telephone hybrid device to your loudspeaker paging system.
4. Administer the switch for the new equipment.

Adjunct information sources

This section lists the documents that you can use to install some key adjunct systems.

You can access or download the latest version of document from the Avaya Support Web site at <http://avaya.com/support>. You must have access to the Internet and a copy of Adobe Reader installed on your personal computer.

To download the latest version of this document:

1. Access the Avaya Support Web site at <http://support.avaya.com>.
2. In the **SEARCH AVAYA SUPPORT** text box, type the document number and click the arrow button.

The system displays the list of document issues. Click the latest version of the document.

Call Management System

For more information about installing Call Management System, see the following documents:

- *Avaya Call Management System (CMS) Software Installation, Maintenance, and Troubleshooting Guide*, 07-300738
- *Avaya Call Management System Sun Fire V880/V890 Computer Hardware Installation, Maintenance, and Troubleshooting*, 585-215-116
- *Avaya Call Management System Sun Blade 100/150 Workstation Hardware Installation, Maintenance, and Troubleshooting*, 585-310-783

Avaya Aura Messaging

For more information about installing Avaya Aura® Modular Messaging systems, see *Avaya Aura® Messaging Release 6 document Library*.

ASAI and DEFINITY LAN Gateway

For more information about installing ASAI systems and DEFINITY LAN Gateway, see *Avaya MultiVantage ASAI Applications over MAPD* (555-230-136) and *Avaya Communication Manager Release 2.0 ASAI Technical Reference* (555-230-220) on the *Avaya Communication Manager Release 2.0 ASAI Documents* CD-ROM (585-246-801).

Another document related to ASAI is *Avaya CVLAN Server 9.0 for Linux Installation and Basic Administration*, which is available at <http://avaya.com/support>.

Avaya Interactive Response

For more information about installing Avaya Interactive Response systems, see *Avaya Interactive Response R1.2.1 Install and Troubleshooting Guide* (07-300180) on the Avaya Interactive Response R1.2.1 document CD (07-300181).

Avaya Extension to Cellular

For more information about installing Avaya Extension to Cellular systems, see the *Avaya Extension to Cellular User's Guide*, 210-100-700.

Property Management Systems

For more information about installing property management systems, see *Guestworks and DEFINITY Systems Technician Handbook for Hospitality Installations*, 555-231-743.

DEFINITY Wireless Business System

For more information about installing DEFINITY Wireless Business System, see *DEFINITY Wireless Business System Installation and Test*, 555-232-102.

Index

Numerical

120A ICSU	96
120A2 ICSU	94
888B converter	111
909A coupler, DC version	116
909A/B universal coupler	115 , 119 , 121 , 122 , 127 , 129
DIP switch settings	116
909B coupler, AC version	116
KS-22911 power supply for	116

A

adapters	
TN2302AP Amphenol adapter	27
adding	
a port network	59
CO trunk	48 , 51
DID trunk	49
DS1 tie trunk	51
FX trunk	48 , 51
ISDN—PRI	56
OPS trunk	51
PCOL trunk	48
tie trunk	49
TN2464BP	46
TN464GP	46
TTC Japanese 2-Mbit trunks	51
WATS trunk	48 , 51
administering	
CDR data collection	80
CDR parameters	81
Expansion Services Module (ESM)	90
external modems	110
IP Media Processor	28
IP Media Resource	38
IPSI	64
loopback jack	96
multimedia call handling (MMCH)	88
multimedia call handling (MMCH) endpoints	89
multimedia call handling (MMCH) one number complex	89
Reliable Data Transport Tool	83
TN799DP C-LAN circuit pack	23
alarm activation level	
setting	64
assigning addresses	60
asynchronous links	92

B

backplane I/O cables, replacing	41
busy tone disconnect	114

C

call detail recording (CDR)	
administering data collection	80
administering parameters	81
connecting equipment	80
testing links	82
calling queue	131
CAMA/E911 trunks	52 , 53 , 54 , 55
circuit packs	
installing	19 , 65
programmable	25
sorted by code	45
TN2183 analog line	130
TN2302AP	25
TN2501	29
TN799DP	20
TNCCSC-1 PRI-to-DASS converter	111 , 113
TNCCSC-2 PRI-to-DPNSS converter	111 , 113
TNPRI/BRI converter	111 , 114
C-LAN	
administering	23
Ethernet adapter	22
installing	21
replacing WP cables with I/O twisted pairs	22
testing external connection to LAN	24
clearing the ARP cache on the laptop	61
CO trunk, adding	48 , 51
coaxial converter, 888B	111
connecting a printer to a G700 or G350 Branch Gateway	92
connections	
CDR equipment	80
ITS	
network	27 , 36
connections, music-on-hold	
FCC-registered equipment	121
non-FCC-registered equipment	121
connectivity	
verifying IPSI	65
Critical Reliability	59 , 64

Index

D

DID trunk	
adding	49
DS1 loopback jack	94
DS1 span	95
T1	94
DS1 tie trunk, adding	51

E

echo cancellation	
with TN2464BP	46
with TN464GP	46
endpoints	88
European Standard Paging Access (ESPA) radio paging equipment	130
Expansion Services Module (ESM)	89
administration	90
installation	90
external communications controller (ECC)	123
external ringing	130

F

Feature Access Code form	54
FX trunk, adding	48 , 51

G

G650 Media Gateway	
installing	59

H

High Reliability.	59 , 64
---------------------------	---

I

I/O cables, replacing	41
installing	
circuit packs	19 , 65
Expansion Services Module (ESM)	90
IOLAN+ 104 terminal server	67
IPSI circuit pack	59
loopback jack.	94
Reliable Data Transport Tool	83
TN2302AP IP Media Processor	26
TN799DP C-LAN	21
integrated channel service unit (ICSU)	94
integration process	
connecting	
ITS to the network	27 , 36

internal communications controller (ICC)	123
IOLAN+ 104 terminal server.	67
installation	67
installing and administering	68

IP address	
assigning	60

IP connectivity hardware	19
------------------------------------	--------------------

IP Media Processor	
administering	28
installing	26
testing external connection to LAN	29
verifying active call status	29

IP Media Resource	
administering	38
testing external connection to LAN	40
verifying active call status	40

IP services	79
-----------------------	--------------------

IPSI	
duplication	64
verifying translations.	65

IPSI circuit pack	60
administering and enabling.	64
assigning IP addresses	60
installing	59
verifying connectivity	65

ISDN adapters	110
-------------------------	---------------------

ISDN converters	110
for multicarrier cabinets	113
for single-carrier cabinets	111
PRI-to-BRI	111 , 114
PRI-to-DASS	111 , 113
PRI-to-DPNSS	111 , 113

ISDN—PRI	
adding	56

K

KS-22911 power supply.	116
KS-22911L2 power supply	119

L

loopback jack	94
administration	96
installation	94

M

main distribution frame (MDF)	130
malicious call trace (MCT).	119
Media Gateway	
G650	59
modems, external	
administration	110

multimedia call handling (MMCH)	87
administering endpoints	89
administering one number complex	89
administering the system	88
connecting endpoints	88
music-on-hold (MOH)	120
connecting FCC-registered equipment	121
connecting non-FCC-registered equipment	121

N

network	
adding a port network	59
ITS	
connecting	27 , 36
network interface	96
node names	78

O

OPS, adding.	51
----------------------	--------------------

P

paging equipment	126
ESPA radio paging	130
external ringing	130
loudspeaker paging for G650 Media Gateways	127
loudspeaker paging for G700 or G350 branch gateways	131
queue warning indicator	131
PCOL trunk, adding	48
printers	
connecting to a G700 or G350 Branch Gateway	92
TCP/IP connections.	92
programmable circuit packs	
TN2302AP	25
TN2464BP	46
TN2501	29
TN464GP	46
TN799DP	20

Q

queue warning indicator	131
-----------------------------------	---------------------

R

Reliability	
Critical	59 , 64
High	59 , 64
Reliable Data Transport Tool (RD TT)	
administering	83
downloading	83

installing	83
----------------------	--------------------

S

switch-to-call accounting link, testing.	82 , 93
--	---

T

T1 DS1 span	94
TCP/IP connections	92
terminal server	67
administering IP node names	78
administering IP services	79
IOLAN+ 104	67
testing, switch-to-call accounting link.	82 , 93
tie trunk	
adding	49
TN2183 analog line circuit pack	130
TN2302AP Amphenol adapter	27
TN2302AP IP Media Processor	25
TN2501 Voice over the LAN circuit pack	29
TN2501AP (integrated announcements)	
faceplate LEDs and interpretation	31
TN2602AP IP Media Resource 320	33
TN429 circuit pack	53
TN799DP C-LAN circuit pack	20
administering	23
installing	21 , 23
TNCCSC-1 PRI-to-DASS converter	111 , 113
TNCCSC-2 PRI-to-DPNSS converter	111 , 113
TNPRI/BRI converter	111 , 114
translations	
verifying IPSI	65
translations, CDR parameters	81 , 93
trunks	
adding	48
CAMA/E911.	52 , 53 , 54 , 55
TTC Japanese 2-Mbit trunks, adding.	51

U

Uniform Call Distribution/Direct Departmental Calling (UCD/DDC) queue	131
---	---------------------

V

VAL See TN2501 Voice over the LAN.	
Voice over LAN	
testing external connection to LAN	33

W

WATS trunk, adding	48 , 51
wideband endpoints	

Index

non-signaling configuration	84
remote port module	86
signaling configuration	85