# Converting Avaya Servers and Gateways

Release 6.2
03-602884
Issue 3
July 2012

**Notice**

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

**Warranty**

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

**Third Party Components**

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

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Licenses**

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

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

**License types**

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

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

**Heritage Nortel Software**

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

**Copyright**

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

**Virtualization**

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. "Instance" means one unique copy of the Software. For example, if the end user customer or Business Partner would like to install 2 instances of the same type of Products, then 2 Products of that type must be ordered.

**How to Get Help**

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

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

**Providing Telecommunications Security**

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

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

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

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

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

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

**Responsibility for Your Company's Telecommunications Security**

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

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

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

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

**TCP/IP Facilities**

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

**Product Safety Standards**

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

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

This product may contain Class 1 laser devices.

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

**Electromagnetic Compatibility (EMC) Standards**

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

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

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

**Federal Communications Commission Part 15 Statement:**

For a Class A digital device or peripheral:

**Note:**

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

For a Class B digital device or peripheral:

**Note:**

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

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

**Equipment With Direct Inward Dialing ("DID"):**

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

**Automatic Dialers:**

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

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

**Toll Restriction and least Cost Routing Equipment:**

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

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

**For equipment approved prior to July 23, 2001:**

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

**For equipment approved after July 23, 2001:**

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

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

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

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

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

**Means of Connection:**

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

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

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

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

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

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

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

**Installation and Repairs**

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

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

**FCC Part 68 Supplier's Declarations of Conformity**

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

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

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

**Canadian Conformity Information**

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

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

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

**European Union Declarations of Conformity**

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

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

**European Union Battery Directive**

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

**Japan**

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

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

**If this is a Class A device:**

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

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

**If this is a Class B device:**

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

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

**Trademarks**

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

Avaya is a registered trademark of Avaya Inc.

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

**Downloading Documentation**

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

**Contact Avaya Support**

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

## Contents

# Chapter 1: Introduction

## Purpose

This document describes procedures for conversions of Avaya telecommunication products that use Avaya Aura® Communication Manager.

## Intended audience

The intended audience of this document are telecommunications managers and telephony administrators.

## Related resources

### Documentation

To help with the procedures in this book, you might need to refer to the following books. The following table lists books contained on the CD-ISO Image of Communication Manager Release 6.2.

| Document Number | Title | Use this document to: | Audience |
|---|---|---|---|
| **Overview** | | | |
| 555-245-772 | *Job Aid: Approved Grounds, (555-245-772)* | Know the description of all approved grounds. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| **Implementing** | | | |

| Document Number | Title | Use this document to: | Audience |
|---|---|---|---|
| 03-603558 | *Implementing Avaya Aura® Communication Manager* | Know procedures to obtain, generate, and retrieve the Communication Manager license and authentication file. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-602885 | *Upgrading to Avaya Aura®Communication Manager* , 03-602885 | Know procedures to upgrade a newer release of software on a server or a newer version of firmware on a hardware component. Components include gateways, media modules, Ethernet switches, and programmable circuit packs. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300686 | *Installing and Connecting the MDF and Telephones, (03-300686)* | Know the procedures to install the main distribution frame and telephones | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300685 | *Installing the Avaya G650 Media Gateway,* (03-300685) | Know the procedures to install a G650 Media Gateway, backplane, and endpoints | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| **Using** | | | |
| 555-245-207 | *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207 | Know the descriptions of all products, components, and connectivity | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-603633 | Avaya Aura® Communication Manager Survivability Options, 03–603633 | Know information on installing and configuring survivable core servers and migrating a main server to an survivable core server. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300509 | *Administering Avaya Aura® Communication Manager*, 03-300509 | Know end-user information on administering trunks and telephones. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |

| Document Number | Title | Use this document to: | Audience |
|---|---|---|---|
| 555-233-504 | *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504 | Know information on implementing converged data and voice communications networks. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300431 | *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431 | Know how to use command interfaces, command syntax, and output from maintenance-related commands. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300430 | *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430 | Know how to use alarms, error codes, and tests to diagnose and repair problems. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| 03-300432 | *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300432 | Know how to troubleshoot and replace various components. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |

# Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

| Course Code | Course title |
|---|---|
| ATI02348IEN, ATI02348VEN | Avaya Aura® Communication Manager Implementation |
| 5U0041I | Avaya Aura® Communication Manager Administration |

## Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

**Note:**

Videos are not available for all products.

## Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

## Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

# Chapter 2: Avaya servers and gateway conversion overview

A conversion is a change in function or mode, reliability, or connectivity of various hardware components. Components include servers and gateways. This document provides module wise information on procedures for Avaya servers and gateway conversion.

A conversion may be preceded by a migration and may include an upgrade.

## Presite checklist

The following checklist lists the information and materials you must collect, and the tasks you must perform, before you can go to the customer site to perform conversion process. Items mentioned in this checklist are common requirements for all conversion modules covered in this document.

| Task | Description |
|---|---|
| Verify that your Services laptop has the appropriate hardware and software. | For more information, see Computer hardware and software requirements on page 16. |
| Verify that your networking settings are correct. | For more information, see Electronic Preinstallation Worksheet on page 19. |
| Verify that your web browser settings are correct | For more information, see Connecting the browser directly to the server on page 18 and Connecting the browser remotely through the network on page 19. |
| Obtain the appropriate logins and passwords for all equipment and software. | For more information, see Logins on page 107. |
| Verify that existing logins do not start with a number or an asterisk (*). | Use Avaya Terminal Emulator or Avaya Site Administration to perform a **`list logins`** command. Linux does not support logins that start with a number or asterisk. |
| Obtain the serial numbers of the gateways and the servers, if necessary. | You need the serial numbers if you are using a new license file or if you are updating an existing license file. |
| Verify that the EPW contains the required, customer-provided network | For more information, see Electronic Preinstallation Worksheet on page 19. |

| Task | Description |
|---|---|
| information. Obtain a completed copy of the Electronic Preinstallation Worksheet (EPW) | |
| Verify that you have the current firmware files. | The software CD-ROM contains firmware for IPSIs, MedPro, C-LAN, and VAL circuit packs. For the most current versions, see Software & Firmware Downloads at http://avaya.com/support. |
| Verify whether you need new license and authentication files. | For more information, see License and authentication files on page 19. |
| Verify that you copied all necessary files to your Services laptop. | You have to copy all the necessary files to your Services laptop. These files include converted translations files, if any, service pack files, a new or updated license file, a new authentication file, and the latest firmware for programmable circuit packs. |
| For Avaya technicians directly connected with their laptop computers, obtain the static craft password that you need to login to the server. | Call the ASG Conversant number, 800-248-1234 or 720-444-5557 and follow the prompts to obtain the password. You need the customer product ID for the FL or IL number. |
| Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary. | Perform this step only if the configuration of the customer INADS alarming modem has changed. |
| Verify that you have the correct cables to connect any new hardware. | For more information, see Computer hardware and software requirements on page 16. |
| Verify that all existing circuit packs work with the new system. | See http://support.avaya.com/CompatibilityMatrix/Index.aspx |
| Verify that you have any new circuit packs that you need to replace older circuit packs. | Replace any TN799B/C C-LAN circuit packs with the TN799DP. |

# Computer hardware and software requirements

The computer that you use to access the server must have following hardware:

- 32-MB of RAM
- 40-MB of available disk space
- A Network interface card (NIC) with a 10/100BaseT Ethernet interface

- A 10/100 BaseT Ethernet, CAT5, cross-connect cable with an RJ45 connector on each end (MDI to MDI-X)
- CD-ROM drive
- Cross-over Ethernet cables
- Direct Ethernet cable
- Serial cable and adapter
- RS-232 port connector
- TN2312BP (IPSI) connection to the Ethernet switches
- TN2302 or TN2306 connection to the LAN

The computer that you use to access the server must have following software:

- Windows 2000 or Windows XP operating system
- HyperTerminal or other terminal emulation program
- TCP/IP networking software, which is bundled with Windows OS
- Web browser: Internet Explorer 7.0 or later or FireFox 3.6 or later

# Configuring the network

### Before you begin

- Note that these instructions are for Windows 2000 and Windows XP only.
- Record any IP addresses, DNS servers, or WINS entries that you change when you configure your services computer. You must restore these entries to connect to other networks.

### About this task

To configure a new network connection, perform the following steps:

### Procedure

1. On your computer desktop, right-click **My Network Places** and left-click **Properties** to display the Network Connections window.

   Windows 2000 and Windows XP automatically detects the Ethernet card in your system and creates a LAN connection for you. More than one connection might occur.
2. Right-click the correct **Local Area Connection** and left-click **Properties** to display the Local Area Connection Properties dialog box.
3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties** to display the Internet Protocol (TCP/IP) Properties dialog box.

5. On the **General** tab, select **Use the following IP address**. Enter the following addresses:
   - IP address: `192.11.13.5`
   - Subnet mask: `255.255.255.252`
6. Record any IP addresses or other entries that you must clear. You might need to restore these later to connect to another network.
7. Select **Use the following DNS server addresses**. Leave the entries for Preferred DNS server and Alternate DNS server blank.
8. At the bottom of the dialog box, click **Advanced** to display the Advanced TCP/IP Settings dialog box.
9. Click the **DNS** tab. Ensure that no DNS server is administered. The address field is blank.
10. Click **OK** > **OK** > **Close** to close all the windows.
11. Reboot the system if directed to do so.

    After you make these changes to the network configuration for your computer, the Network and Dial-up Connections window shows the status of the Local Area Connection. The system displays:
    - `Enabled` when the Ethernet cable from the laptop is connected to the server.
    - `Disabled` or `unplugged` when the NIC is not connected to any other equipment.

# Connecting the browser directly to the server

## About this task

**Note:**

Instructions are for Internet Explorer 7.0 only.

## Procedure

1. Click **Tools** > **Internet Options**.
2. Click the **Connection** tab.
3. In the LAN Settings box in the lower right hand of the page, click **Advanced**.
4. In the Exceptions box after the last entry, type `192.11.13.6`

5. Click **OK** > **OK** > **OK** again to close all the dialog boxes.

## Connecting the browser remotely through the network

### About this task

When you connect through a proxy server, a connection session to a server can time out. To avoid a server time out during a session, add the host names or the IP addresses of the servers to the list of host names and IP addresses.

To add the host names or the IP addresses of the servers to the list of host names and IP addresses:

**Note:**

The following instructions are for Internet Explorer 7.0 only.

### Procedure

1. Click **Tools** > **Internet Options**.
2. Click the **Connection** tab.
3. Click **LAN settings** > **Advanced**.
4. In the **Do not use proxy server for addresses beginning with** field, type the IP address for each server that you want to access remotely. If the first or the first and second octets are the same, you can shorten the address to xxx.xxx.* For example, if you have the IP addresses 135.9.42.75 and 135.9.113.113, then you can type `135.9.*`.
5. Click **OK** > **OK** > **OK** again to close all the dialog boxes.

## Electronic Preinstallation Worksheet

The Electronic Preinstallation Worksheet (EPW) is an Excel spreadsheet. The EPW provides the customer network information that you need to use the Avaya Installation Wizard to configure the control network components. You can obtain the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at http://support.avaya.com/avayaiw/.

## License and authentication files

You must install a new or an updated license file if you:

- Are changing the mode of the server, including:
  - S8300D survivable remote server to main server
  - S8510 or S8800 main to survivable core server or survivable core server to main
  - S8510 or S8800 MBS to survivable core server
- Are installing TN2602AP Media Resource 320 circuit packs. The license file specifies the maximum number of available voice channels.
- Also need to install a new license file and a new authentication file because you are adding new purchased features.

For more information on how to obtain license and authentication files, see *Implementing Avaya Aura® Communication Manager, 03–603558*.

# Performing preconversion tasks

### Procedure

1. Redesign the networks. For more information, see *Redesigning the networks*.
2. Create and update the license and the authentication files from the PLDS website.
3. Obtain the postconversion service pack file, if any. For more information, see *Obtaining the postconversion service pack file*.

# Redesigning the networks

### About this task

To redesign the network, perform the following tasks:

### Procedure

1. Assess the impact of the main server to survivable remote server conversion on all voice and voice messaging network nodes.
2. Plan for any necessary changes to network elements.
3. Collect the following primary server configuration information for the new survivable remote server:
   - host name and IP address
   - main server IP address(es)
   - DNS IP addresses (if used)

- UPS IP addresses (if used)
- static routes data (if used)
- time server data
- modem return route data (if supported by Avaya Services)

## Obtaining the postconversion service pack file

### Procedure

1. Go to http://support.avaya.com and click **Downloads** to see if there is a service pack file available for the Communication Manager release you are currently running, for example, release 6.2, load 628.0
2. If a service pack file is available, download it and take it to the customer site.

# Reliability and availability

The reliability of a telecommunications system is defined by the extent of duplication of certain components. For Linux-based servers, the standard reliability level includes single server for S8510, S8800, HP DL360 G7, and Dell R610 servers, and duplicated server for S8800, HP DL360 G7, and Dell R610 servers.

The availability of a telecommunications system is the time the system is ready and able to process calls as a percentage of the scheduled time. Availability depends on reliability.

The standard feature also provides the ability to combine types of port network connectivity (PNC) and to apply reliability designations to the IP-PNC portion of the system. The reliability level is defined per port network for the IP-PNC portion. Therefore, combined PNC systems can have combined reliabilities. For pure IP-PNC configurations, the reliability designation is also per port network.

The standard feature also provides the ability to add, to an IP-PNC port network, duplicated bearer reliability, in addition to duplicated control reliability, which together constitute critical reliability.

The following table summarizes reliability levels for systems with Linux-based servers. Reliability definitions for pre-Linux-based CSI switch are unchanged.

**Note:**

The terms control and bearer mean control network and bearer network, respectively. More detailed definitions of reliability levels, including the circuit packs involved, are given in the

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

| Server Name | Single Server | Duplicated Server |
|---|---|---|
| S8510-Series Server | • One server<br>• Single control<br>• Single/duplicated bearer | NA |
| S8510-Series Server with Processor Ethernet connectivity to H.248 Branch Gateways | • One server<br>• Single control<br>• Single/duplicated bearer | NA |
| S8800/HP DL360 G7/Dell R610-Series Server | • One server<br>• Single control<br>• Single/duplicated bearer | • two servers<br>• single/duplicated control<br>• single/duplicated bearer |
| S8800/HP DL360 G7/Dell R610-Series Server (Duplicated Ethernet and IP connected H.248 Branch Gateways) | NA | • two servers<br>• duplicated control<br>• duplicated bearer |

# Chapter 3: Conversion of S8300D main server mode to S8300D survivable remote server mode

This chapter provides a high-level list of tasks for converting an S8300D main server to survivable remote server mode by changing the Communication Manager template. To complete these tasks, see *Implementing Avaya Aura® Communication Manager, 03–603558*.

In this scenario, an S8300D, configured as a main server, is converted to an S8300D server in the survivable remote server mode. During the process of conversion, the CM_onlyEmbed template is removed and CM_SurvRemote template is installed to convert the main server to the survivable remote server.

## Converting S8300D main server to S8300D survivable remote server

### Before you begin

Ensure that you have followed all the necessary steps mentioned in Performing preconversion tasks on page 20.

### About this task

**Note:**

It is important to note where the task is performed. Most of the tasks are done on a server or gateway — on the main server/survivable remote server S8300D, on the main server for the survivable remote server, on a DHCP server, or on the gateway processor (MGP).

### Procedure

1. On the main server of the new survivable remote server, perform the following:
   a. Administer the main server that the survivable remote server will use (after conversion). See *Administering the main server that the survivable remote server will use*.
   b. Administer the gateway. See *Administering the gateway*.
   c. Reassign endpoints from the main server to this main server. See *Reassigning endpoints from the main server to this main server*.

2. On the DHCP server, update the alternate controller list on the DHCP server.
3. On the MGP of the gateway, go to the MGP command prompt and change the controller list of the gateway. See *Changing the gateway's controller list*.
4. On the main server of the survivable remote server, verify that the gateway has registered with the main server. See *Verifying gateway registration with the main server*.
5. On the main server and survivable remote server, do the following:
   a. Configure the main server. See *Configuring the main server and survivable remote server*.
   b. Configure the survivable remote server. See *Configuring the main server and survivable remote server*.
6. On the main server of the survivable remote server, do the following:
   a. verify survivable remote server status. See *Verifying survivable remote server status*.
   b. If the translations of the survivable remote server have not synchronized with the main server, invoke translation synchronization. See *Invoking translation synchronization*.

# Administering the main server that the survivable remote server will use after conversion

### About this task

To administer the main server that the survivable remote server will use (after conversion), perform the following steps:

### Procedure

1. Assign node names.
2. Administer network regions.
3. Associate survivable remote server with a network region.
4. Administer IP interfaces.
5. Identify survivable remote servers to the main server.

## Administering the gateway while converting S8300D survivable remote server mode to S8300D main server mode

### About this task

To administer the gateway, perform the following steps:

### Procedure

1. Add gateway.
2. Repeat for each gateway controlled by the current main server.
3. For this scenario, the gateway will not automatically register with the main server at this point. Skip the subtasks Verify Changes and Save Translations in this section.
4. When the gateway finally registers, the media modules will automatically populate, unless you are doing Administration Without Hardware (AWOH). In this case, you will have to enter the media module types for each slot.

## Reassigning endpoints from the main server to this main server

### About this task

To reassign endpoints from the main server to this main server, perform the following steps:

### Procedure

1. Update translations — add stations and trunks.
   a. If the main server is a new installation, using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
   b. Alternatively, use SAT commands.
2. Place test calls to verify.
3. Reassign Communication Manager Messaging users to the messaging system used by this main server. Enter test messages to verify.

## Changing the controller list of gateway while converting S8300D survivable remote server mode to S8300D main server mode

### About this task

To change the controller list of gateway, perform the following steps:

### Procedure

1. Clear the controller list of the gateway.
2. Enter the IP addresses of the main server and up to three alternate controllers.
3. Set the survivable remote server transition points.
4. To start the gateway, run the command **`copy running-config startup-config`**.
5. Reset MGP.

## Verifying gateway registration with the main server

### About this task

To verify gateway registration with the main server, perform the following steps:

### Procedure

1. Open a SAT session and enter list media-gateway. Verify that the **Registered** field (Reg?) is set to y.
2. Place a test call.

## Configuring the main server and survivable remote server

### About this task

To configure the main server and survivable remote server, perform the following steps:

### Procedure

1. If Communication Manager Messaging is installed, get Communication Manager Messaging data and stop Communication Manager Messaging.
2. Record configuration information.

a. If you have not already done so, in the Record Configuration Information task, record all of the configuration information.
b. Re-enter some of this information after the conversion.

3. Remove CM_onlyEmbed template.
4. Install CM_SurvRemoteEmbed template.
5. Set time, date, and time zone.

**Note:**

The time of the survivable remote server must be set to the same time zone as its main server, even if the survivable remote server is physically located in a different time zone.

6. Install postconversion service pack file, if any.
7. Install the new authentication file, if required.
8. Configure server.
   a. Fill in each Server Configuration screen with data for the survivable remote server. Some of the configuration data will be the same as that for the main server.
   b. On the Server Role window, select the radio button that indicates this is NOT a main server.
9. Reboot the survivable remote server.
   a. Open a SAT session and enter `reset system 4`.
   b. After the reboot, the survivable remote server should be registered with the main server and in a few minutes translations should be synchronized.

# Verifying survivable remote server status

### About this task

To verify survivable remote server status, perform the following steps:

### Procedure

1. At the SAT prompt, enter `list survivable-processor` (for Avaya Aura® CM R3.1) or `list lsp` (for Avaya Aura® CM R2.x). The survivable remote server name and IP address should be listed.
2. To view the translations dates and times of the main server, enter `list configuration software-version`.

3. Ensure that the Translations Updated date and time is matching the translations date and time on the main server.

## Invoking translation synchronization while converting S8300D survivable remote server mode to S8300D main server mode

### About this task

To invoke translation synchronization, perform the following steps:

### Procedure

1. On the main server, enter the Linux command `filesync -a` *ipaddress*, where *ipaddress* is the IP address of the survivable remote server.
2. Ensure that the translation synchronization completed successfully. Wait several minutes.
3. Check the timestamp of the survivable remote server translation files with the SAT command **`list survivable-processor`** or **`list lsp`** on the main server.

# Performing postconversion tasks to convert S8300D main server mode to S8300D survivable remote server mode

### About this task

After conversion, you need to carry out the following tasks:

### Procedure

1. Implement any additional design changes to voice and/or voice messaging networks.
2. Re-register the S8300D Server as a survivable remote server with the Avaya remote servicing center.

# Chapter 4: Conversion of S8300D survivable remote server mode to S8300D main server mode

This chapter provides a high-level list of tasks for converting an S8300D survivable remote server mode to main server mode by changing the Communication Manager template. To complete these tasks, see *Implementing Avaya Aura® Communication Manager, 03–603558*.

In this scenario, an S8300D, configured as a survivable remote server, is converted to an S8300D standalone main server. During the process of conversion, the CM_SurvRemoteEmbed template used for survivable remote server is removed and the CM_onlyEmbed template of the 6.2 version is installed, to convert the survivable remote server to a main server.

## Converting S8300D survivable remote server to S8300D main server

### Before you begin

Ensure that you have followed all the necessary steps mentioned in Performing preconversion tasks on page 20.

### About this task

To convert the S8300D survivable remote server to S8300D main server, perform the following tasks at the customer site.

**Note:**

It is important to note where the task is performed. Most of the tasks are done on a server or gateway — on the main server/survivable remote server S8300D, on the main server for the survivable remote server, on a DHCP server, or on the gateway processor (MGP).

### Procedure

1. On the main server of the new survivable remote server, do the following:
   a. Administer the main server to which the survivable remote server was formerly assigned. See *Administering the main server to which the survivable remote server was formerly assigned*.
   b. Administer the gateway. See *Administering the gateway*.

c. Reassign endpoints from the main server to this main server. See *Reassigning endpoints from the main server to this main server*.

2. On the DHCP server, update the alternate controller list on the DHCP server.
3. On the MGP of the gateway, go to the MGP command prompt and change the gateway's controller list. See *Changing the gateway's controller list*.
4. On the survivable remote server to be converted, configure the parameters. See *Configuring the survivable remote server to be converted*.
5. On the main server of the survivable remote server, remove endpoints that will be controlled by the new main server from the current main server.
6. On the new main server, verify that the gateway has registered with the main server. See *Verifying gateway registration with the main server*.
7. On survivable remote servers of the new main server (if any), do the following:
   a. Reboot survivable remote servers (if any). See *Rebooting survivable remote servers*.
   b. Verify survivable remote server translations date and time (if any). See *Verifying survivable remote server translations date and time*.
8. On the main server, do the following:
   a. verify survivable remote server status. See *Verifying survivable remote server status*.
   b. If the translations of the survivable remote server have not synchronized with the main server, invoke translation synchronization. See *Invoking translation synchronization*.

# Administering the main server to which the survivable remote server was formerly assigned

## About this task

To administer the main server to which the survivable remote server was formerly assigned, perform the following steps:

## Procedure

1. Remove survivable remote server node name with the **`change node-names ip`** command.
2. Disassociate survivable remote server from network regions with the **`change ip-network-region`** *number* command.
3. Remove survivable remote server from the survivable remote server screen with the **`remove survivable-processor`** *node-name* command.

4. Repeat for every survivable remote server to be controlled by the new main server.

## Administering the gateway

### About this task

To administer the gateway, perform the following steps:

### Procedure

1. Remove gateway with the **`remove media-gateway`** *number* command.
2. Repeat for each gateway to be controlled by the converted survivable remote server.

## Reassigning endpoints from the main server to this main server

### About this task

To reassign endpoints from the main server to this main server, perform the following steps:

### Procedure

1. Update translations — add stations and trunks.
   a. If the main server is a new installation, using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
   b. Alternatively, use SAT commands.
2. Place test calls to verify.
3. Reassign Communication Manager Messaging users to the messaging system used by this main server. Enter test messages to verify.

## Changing the controller list of gateway

### About this task

To change the gateway controller list, perform the following steps:

### Procedure

1. Clear the controller list of the gateway.
2. Enter the IP addresses of the new main server and up to three alternate controllers.
3. To start the gateway, run the command **`copy running-config startup-config`**.
4. Reset MGP.

## Configuring the survivable remote server to be converted

### About this task

To configure the survivable remote server to be converted, perform the following steps:

### Procedure

1. Backup all system files — translations, OS, and security backup sets.

   These backup sets will not be restored on the S8300D server. They should be backed up in case it is necessary to revert to the original configuration.
2. Record configuration information.

   If you have not already done so, in the Record Configuration Information task, record all of the configuration information. Re-enter some of this information after the conversion.
3. Remove the CM_SurvRemoteEmbed template
4. Install the CM_onlyEmbed template.
5. Enable Communication Manager Messaging, if required.
6. Set time, date, and time zone.

   You have to set the time zone of the new main server. All survivable remote servers under the control of the main server must be set to the time zone of the new main server.
7. Install postconversion service pack file, if any.
8. Install the new main server license file.
9. Install the new authentication file, if required.
10. Configure server.
    a. Fill in each Server Configuration screen with data for the main server. Some of the configuration data will be the same as that for the survivable remote server.

b. On the Server Role screen, select the radio button that indicates this is NOT a survivable remote server.

11. Administer the new main server.
    a. Assign node names.
    b. Administer network regions.
    c. Associate other survivable remote servers (if any) with a network region.
    d. Add IP interfaces.
    e. Identify survivable remote servers to the main server.
12. Administer the gateway.
    a. Add gateway.
    b. Repeat for each gateway to be controlled by the new main server.
    c. For this scenario, the gateway will not automatically register with the main server at this point. Skip the subtasks, Verify Changes and Save Translations in this section.
    d. When the gateway finally registers, the media modules will automatically populate, unless you are doing administration without hardware (AWOH). In this case, you will have to enter the media module types for each slot.
13. Reassign endpoints from the current main server to the standalone main server.
    a. Update translations — add stations and trunks
        • Using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
        • Alternatively, use SAT commands.
    b. Place test calls to verify.
    c. Reassign messaging system users of the current main server to the messaging system used by the new main server. Enter test messages to verify.
14. Reboot the main server.

# Verifying gateway registration with the main server

### About this task

To verify gateway registration with the main server, perform the following steps:

### Procedure

1. Open a SAT session and enter list media-gateway. Verify that the **Registered** field (Reg?) is set to y.
2. Place a test call.

# Configuring the main server and the survivable remote server to convert S8300D survivable remote server to S8300D main server

## About this task

To configure the main server and survivable remote server, perform the following steps:

## Procedure

1. If Communication Manager Messaging is installed, get Communication Manager Messaging data and stop Communication Manager Messaging.
2. Record configuration information.
   a. If you have not already done so, in the Record Configuration Information task, record all of the configuration information.
   b. Re-enter some of this information after the conversion.
3. Remove CM_onlyEmbed template.
4. Install CM_SurvRemoteEmbed template.
5. Set time, date, and time zone.

   **Note:**

   The time of the survivable remote server must be set to the same time zone as its main server, even if the survivable remote server is physically located in a different time zone.
6. Install postconversion service pack file, if any.
7. Install the new authentication file, if required.
8. Configure server.
   a. Fill in each Server Configuration screen with data for the survivable remote server. Some of the configuration data will be the same as that for the main server.
   b. On the Server Role window, select the radio button that indicates this is NOT a main server.
9. Reboot the survivable remote server.
   a. Open a SAT session and enter `reset system 4`.
   b. After the reboot, the survivable remote server should be registered with the main server and in a few minutes translations should be synchronized.

## Verifying survivable remote server status

### About this task

To verify survivable remote server status, perform the following steps:

### Procedure

1. At the SAT prompt, enter `list survivable-processor` (for Avaya Aura® CM R3.1) or `list lsp` (for Avaya Aura® CM R2.x). The survivable remote server name and IP address should be listed.
2. To view the translations dates and times of the main server, enter `list configuration software-version`.
3. Ensure that the Translations Updated date and time is matching the translations date and time on the main server.

## Invoking translation synchronization

### About this task

To invoke translation synchronization, perform the following steps:

### Procedure

1. On the main server, enter the Linux command `filesync -a trans`.
2. Ensure that the translation synchronization completed successfully. Wait several minutes.
3. Check the timestamp of the survivable remote server translation files with the SAT command **`list survivable-processor`** or **`list lsp`** on the main server.

# Performing postconversion tasks to convert S8300D survivable remote server to S8300D main server

## Procedure

Implement any additional design changes to voice and/or voice messaging networks.

# Chapter 5: Conversion of S8510/S8800/HP DL360 G7/Dell R610 main server mode to S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode (CM_Simplex template)

This chapter provides a high-level list of tasks for converting an S8510/S8800/HP DL360 G7/Dell R610 main server to survivable remote server mode by changing the Communication Manager template. To complete these tasks, see *Implementing Avaya Aura® Communication Manager, 03–603558*.

In this scenario, an S8510/S8800//HP DL360 G7/Dell R610, configured as a main server, is converted to an S8510/S8800//HP DL360 G7/Dell R610 in survivable remote server mode.

## Converting S8510/S8800/HP DL360 G7/Dell R610 main server mode to S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode (CM_Simplex Template)

### Before you begin

Ensure that you have followed all the necessary steps mentioned in Performing preconversion tasks on page 20.

### About this task

To convert the S8510/S8800/HP DL360 G7/Dell R610 main server mode to S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode (CM_Simplex Template), perform the following tasks at the customer site.

**Note:**

It is important to note where the task is performed. Most of the tasks are done on a server or gateway — on the main server/survivable remote server, on the main server for the survivable remote server, on a DHCP server, or on the gateway processor (MGP).

### Procedure

1. On the main server of the new survivable remote server, do the following:
   a. Administer the main server to which the survivable remote server was formerly assigned. See *Administering the main server to which the survivable remote server was formerly assigned*.
   b. Administer the gateway. See *Administering the gateway*.
   c. Reassign endpoints from the main server to this main server. See *Reassigning endpoints from the main server to this main server*.
2. On the DHCP server, update the alternate controller list on the DHCP server.
3. On the MGP of the gateway, go to the MGP command prompt and change the gateway's controller list. See *Changing the gateway's controller list*.
4. On the survivable remote server to be converted, take a backup of all system files: translations, OS, and security backup sets.

   **Note:**

   These backup sets will not be restored on the S8510/S8800/HP DL360 G7/Dell R610. They should be backed up in case it is necessary to revert to the original configuration.
5. On the main server/survivable remote server, configure the parameters. See *Configuring the main server and the survivable remote server*.
6. On the main server, do the following:
   a. verify survivable remote server status. See *Verifying survivable remote server status*.
   b. If the translations of the survivable remote server have not synchronized with the main server, invoke translation synchronization. See *Invoking translation synchronization*.

## Administering the main server to which the survivable remote server was formerly assigned

### About this task

To administer the main server to which the survivable remote server was formerly assigned, perform the following steps:

### Procedure

1. Remove survivable remote server node name with the **`change node-names ip`** command.

2. Disassociate survivable remote server from network regions with the **`change ip-network-region`** *number* command.
3. Remove survivable remote server from the survivable remote server screen with the **`remove survivable-processor`** *node-name* command.
4. Repeat for every survivable remote server to be controlled by the new main server.

## Administering the gateway

### About this task

To administer the gateway, perform the following steps:

### Procedure

1. Remove gateway with the **`remove media-gateway`** *number* command.
2. Repeat for each gateway to be controlled by the converted survivable remote server.

## Reassigning endpoints from the main server to this main server

### About this task

To reassign endpoints from the main server to this main server, perform the following steps:

### Procedure

1. Update translations — add stations and trunks.
   a. If the main server is a new installation, using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
   b. Alternatively, use SAT commands.
2. Place test calls to verify.
3. Reassign Communication Manager Messaging users to the messaging system used by this main server. Enter test messages to verify.

# Changing the controller list of gateway

### About this task

To change the gateway controller list, perform the following steps:

### Procedure

1. Clear the controller list of the gateway.
2. Enter the IP addresses of the new main server and up to three alternate controllers.
3. To start the gateway, run the command **`copy running-config startup-config`**.
4. Reset MGP.

# Configuring the main server and the survivable remote server to convert S8510/S8800/HP DL360 G7/Dell R610 main server mode to S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode (CM_Simplex Template)

### About this task

To configure the main server and survivable remote server, perform the following steps:

### Procedure

1. If Communication Manager Messaging is installed, get Communication Manager Messaging data and stop Communication Manager Messaging.
2. Record configuration information.
   a. If you have not already done so, in the Record Configuration Information task, record all of the configuration information.
   b. Re-enter some of this information after the conversion.
3. Change the server role to survivable remote server.
   a. On the System Management Interface (SMI), go to **Administration**, and then click **Server (Maintenance)**.
   b. Under **Server Configuration**, click **Server Role**, and then select the radio button that indicates this is Survivable remote server (Local Survivable Processor (LSP)).
4. Install CM_SurvRemoteEmbed template.

5. Set time, date, and time zone.

   **Note:**

   The time of the survivable remote server must be set to the same time zone as its main server, even if the survivable remote server is physically located in a different time zone.

6. Install postconversion service pack file, if any.
7. Install the new authentication file, if required.
8. Reboot the survivable remote server.
   a. Open a SAT session and enter `reset system 4`.
   b. After the reboot, the survivable remote server should be registered with the main server and in a few minutes translations should be synchronized.

## Verifying survivable remote server status

### About this task

To verify survivable remote server status, perform the following steps:

### Procedure

1. At the SAT prompt, enter `list survivable-processor` (for Avaya Aura® CM R3.1) or `list lsp` (for Avaya Aura® CM R2.x). The survivable remote server name and IP address should be listed.
2. To view the translations dates and times of the main server, enter `list configuration software-version`.
3. Ensure that the Translations Updated date and time is matching the translations date and time on the main server.

## Invoking translation synchronization

### About this task

To invoke translation synchronization, perform the following steps:

### Procedure

1. On the main server, enter the Linux command `filesync -a trans`.

2. Ensure that the translation synchronization completed successfully. Wait several minutes.
3. Check the timestamp of the survivable remote server translation files with the SAT command **`list survivable-processor`** or **`list lsp`** on the main server.

# Performing postconversion tasks to convert S8510/ S8800/HP DL360 G7/Dell R610 main server mode to S8510/ S8800/HP DL360 G7/Dell R610 survivable remote server mode (CM_Simplex Template)

### About this task

After conversion, you need to carry out the following tasks:

### Procedure

1. Implement any additional design changes to voice and/or voice messaging networks.
2. Reregister the new survivable remote server with the Avaya remote servicing center.

# Chapter 6: Conversion of S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/ S8800/HP DL360 G7/Dell R610 main server mode (CM_Simplex template)

This chapter provides a high-level list of tasks for converting an S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to main server mode without changing the Communication Manager template. To complete these tasks, see *Implementing Avaya Aura® Communication Manager, 03–603558*.

In this scenario, an S8510/S8800/HP DL360 G7/Dell R610, configured as a survivable remote server, is converted to an S8510/S8800//HP DL360 G7/Dell R610 in main server mode.

**Note:**

For the installation and conversion procedures in this chapter use the System Management Interface (SMI) for Release 6.2. Some of the tasks can be automated by using the Avaya Installation Wizard with the Electronic Preinstallation Worksheet (EPW).

## Converting S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/S8800/HP DL360 G7/Dell R610 main server mode (CM_Simplex template)

### Before you begin

Ensure that you have followed all the necessary steps mentioned in Performing preconversion tasks on page 20.

### About this task

To convert the S8510/S8800/HP DL360 G7/Dell R610 main server mode to S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode (Avaya Aura® CM_Simplex Template), perform the following tasks at the customer site.

**Note:**

It is important to note where the task is performed. Most of the tasks are done on a server or gateway — on the main server/survivable remote server, on the main server for the survivable remote server, on a DHCP server, or on the gateway processor (MGP).

### Procedure

1. On the main server of the new survivable remote server, do the following:
   a. Administer the main server to which the survivable remote server was formerly assigned. See *Administering the main server to which the survivable remote server was formerly assigned*.
   b. Administer the gateway. See *Administering the gateway*.
   c. Reassign endpoints from the main server to this main server. See *Reassigning endpoints from the main server to this main server*.
2. On the DHCP server, update the alternate controller list on the DHCP server.
3. On the MGP of the gateway, go to the MGP command prompt and change the gateway's controller list. See *Changing the gateway's controller list*.
4. On the survivable remote server to be converted, take a backup all system files: translations, OS, and security backup sets.

   **Note:**

   These backup sets will not be restored on the S8510/S8800/HP DL360 G7/Dell R610. They should be backed up in case it is necessary to revert to the original configuration.
5. On the main server/survivable remote server, configure the parameters. See Configuring the main server and the survivable remote server.

## Administering the main server to which the survivable remote server was formerly assigned

### About this task

To administer the main server to which the survivable remote server was formerly assigned, perform the following steps:

### Procedure

1. Remove survivable remote server node name with the **`change node-names ip`** command.
2. Disassociate survivable remote server from network regions with the **`change ip-network-region`** *number* command.

3. Remove survivable remote server from the survivable remote server screen with the **`remove survivable-processor`** *node-name* command.
4. Repeat for every survivable remote server to be controlled by the new main server.

## Administering the gateway

### About this task

To administer the gateway, perform the following steps:

### Procedure

1. Remove gateway with the **`remove media-gateway`** *number* command.
2. Repeat for each gateway to be controlled by the converted survivable remote server.

## Reassigning endpoints from the main server to this main server

### About this task

To reassign endpoints from the main server to this main server, perform the following steps:

### Procedure

1. Update translations — add stations and trunks.
   a. If the main server is a new installation, using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
   b. Alternatively, use SAT commands.
2. Place test calls to verify.
3. Reassign Communication Manager Messaging users to the messaging system used by this main server. Enter test messages to verify.

## Changing the controller list of gateway

### About this task

To change the gateway controller list, perform the following steps:

### Procedure

1. Clear the controller list of the gateway.
2. Enter the IP addresses of the new main server and up to three alternate controllers.
3. To start the gateway, run the command **`copy running-config startup-config`**.
4. Reset MGP.

# Configuring the main server and the survivable remote server to convert S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/S8800/HP DL360 G7/Dell R610 main server mode (CM_Simplex template)

### About this task

To configure the main server and survivable remote server, perform the following steps:

### Procedure

1. Record configuration information.
   a. If you have not already done so, in the Record Configuration Information task, record all of the configuration information.
   b. Reenter some of this information after the conversion.
2. Change the server role to main server.
   a. On the System Management Interface (SMI), go to **Administration**, and then click **Server (Maintenance)**.
   b. Under **Server Configuration**, click **Server Role**, and then select the radio button that indicates this is the main server.
   c. Fill in each Server Configuration screen with data for the main server. Some of the configuration data will be the same as that for the survivable remote server.
3. Enable Communication Manager Messaging, if required.
4. Set time, date, and time zone.

   **Note:**

   The time of the survivable remote server must be set to the same time zone as its main server, even if the survivable remote server is physically located in a different time zone.

5. Install postconversion service pack file, if any.
6. Install the new main server license file.
7. Install the new authentication file, if required.
8. Administer the new main server.
    a. Assign node names.
    b. Administer network regions.
    c. Associate other survivable remote servers (if any) with a network region.
    d. Add IP interfaces.
    e. Identify survivable remote servers to the main server.
9. Administer the gateway.
    a. Add gateway.
    b. Repeat for each gateway to be controlled by the new main server.
    c. For this scenario, the gateway will not automatically register with the main server at this point. Skip the subtasks, Verify Changes and Save Translations in this section.
    d. When the gateway finally registers, the media modules will automatically populate, unless you are doing administration without hardware (AWOH). In this case, you will have to enter the media module types for each slot.
10. Reassign endpoints from the current main server to the standalone main server.
    a. Update translations — add stations and trunks
        - Using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
        - Alternatively, use SAT commands.
    b. Place test calls to verify.
    c. Reassign messaging system users of the current main server to the messaging system used by the new main server. Enter test messages to verify.
11. Reboot the survivable remote server.
    a. Open a SAT session and enter `reset system 4`.
    b. After the reboot, the survivable remote server should be registered with the main server and in a few minutes translations should be synchronized.

# Chapter 7: Conversion of S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/ S8800/HP DL360 G7/Dell R610 main server mode (CM_SurvRemote to CM_Simplex)

This chapter provides a high-level list of tasks for converting an S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to main server mode by changing the Communication Manager template. To complete these tasks, see *Implementing Avaya Aura® Communication Manager*.

In this scenario, an S8510/S8800//HP DL360 G7/Dell R610, configured as a survivable remote server, is converted to an S8510/S8800//HP DL360 G7/Dell R610 in main server mode.

**Note:**

For the installation and conversion procedures in this chapter use the System Management Interface (SMI) for Release 6.2. Some of the tasks can be automated by using the Avaya Installation Wizard with the Electronic Preinstallation Worksheet (EPW).

## Converting S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/S8800/HP DL360 G7/Dell R610 main server mode (CM_SurvRemote to CM_Simplex)

### Before you begin

Ensure that you have followed all the necessary steps mentioned in Performing preconversion tasks on page 20.

### About this task

To convert the S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/S8800/HP DL360 G7/Dell R610 main server mode (CM_SurvRemote to CM_Simplex), perform the following tasks at the customer site.

**Note:**

It is important to note where the task is performed. Most of the tasks are done on a server or gateway — on the main server/survivable remote server, on the main server for the survivable remote server, on a DHCP server, or on the gateway processor (MGP).

### Procedure

1. On the main server of the new survivable remote server, do the following:
   a. Administer the main server to which the survivable remote server was formerly assigned. See *Administering the main server to which the survivable remote server was formerly assigned*.
   b. Administer the gateway. See *Administering the gateway*.
   c. Reassign endpoints from the main server to this main server. See *Reassigning endpoints from the main server to this main server*.
2. On the DHCP server, update the alternate controller list on the DHCP server.
3. On the MGP of the gateway, go to the MGP command prompt and change the gateway's controller list. See *Changing the gateway's controller list*.
4. On the survivable remote server to be converted, take a backup of all system files: translations, OS, and security backup sets.

   **Note:**

   These backup sets will not be restored on the S8510/S8800/HP DL360 G7/Dell R610. They should be backed up in case it is necessary to revert to the original configuration.
5. On the main server/survivable remote server, configure the parameters. See *Configuring the main server and the survivable remote server*.

## Administering the main server to which the survivable remote server was formerly assigned

### About this task

To administer the main server to which the survivable remote server was formerly assigned, perform the following steps:

### Procedure

1. Remove survivable remote server node name with the **change node-names ip** command.
2. Disassociate survivable remote server from network regions with the **change ip-network-region** *number* command.
3. Remove survivable remote server from the survivable remote server screen with the **remove survivable-processor** *node-name* command.
4. Repeat for every survivable remote server to be controlled by the new main server.

## Administering the gateway

### About this task

To administer the gateway, perform the following steps:

### Procedure

1. Remove gateway with the **remove media-gateway** *number* command.
2. Repeat for each gateway to be controlled by the converted survivable remote server.

## Reassigning endpoints from the main server to this main server

### About this task

To reassign endpoints from the main server to this main server, perform the following steps:

### Procedure

1. Update translations — add stations and trunks.
   a. If the main server is a new installation, using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
   b. Alternatively, use SAT commands.
2. Place test calls to verify.
3. Reassign Communication Manager Messaging users to the messaging system used by this main server. Enter test messages to verify.

## Changing the controller list of gateway

### About this task

To change the gateway controller list, perform the following steps:

### Procedure

1. Clear the controller list of the gateway.
2. Enter the IP addresses of the new main server and up to three alternate controllers.
3. To start the gateway, run the command **`copy running-config startup-config`**.
4. Reset MGP.

## Configuring the main server and the survivable remote server to convert S8510/S8800/HP DL360 G7/Dell R610 survivable remote server mode to S8510/S8800/HP DL360 G7/Dell R610 main server mode (CM_SurvRemote to CM_Simplex)

### About this task

To configure the main server and survivable remote server, perform the following steps:

### Procedure

1. Record configuration information.
   a. If you have not already done so, in the Record Configuration Information task, record all of the configuration information.
   b. Reenter some of this information after the conversion.
2. Remove the CM_SurvRemote template.
3. Install the CM_Simplex template.
4. Change the server role to main server.
   a. On the System Management Interface (SMI), go to **Administration**, and then click **Server (Maintenance)**.
   b. Under **Server Configuration**, click **Server Role**, and then select the radio button that indicates this is the Main server.

c. Fill in each Server Configuration screen with data for the main server. Some of the configuration data will be the same as that for the survivable remote server.

5. Enable Communication Manager Messaging, if required.
6. Set time, date, and time zone.

**Note:**

The time of the survivable remote server must be set to the same time zone as its main server, even if the survivable remote server is physically located in a different time zone.

7. Install postconversion service pack file, if any.
8. Install the new main server license file.
9. Install the new authentication file, if required.
10. Administer the new main server.
    a. Assign node names.
    b. Administer network regions.
    c. Associate other survivable remote servers (if any) with a network region.
    d. Add IP interfaces.
    e. Identify survivable remote servers to the main server.
11. Administer the gateway.
    a. Add gateway.
    b. Repeat for each gateway to be controlled by the new main server.
    c. For this scenario, the gateway will not automatically register with the main server at this point. Skip the subtasks, Verify Changes and Save Translations in this section.
    d. When the gateway finally registers, the media modules will automatically populate, unless you are doing administration without hardware (AWOH). In this case, you will have to enter the media module types for each slot.
12. Reassign endpoints from the current main server to the standalone main server.
    a. Update translations — add stations and trunks
        - Using the Avaya Installation Wizard and the Electronic Preinstallation Worksheet (EPW) is recommended.
        - Alternatively, use SAT commands.
    b. Place test calls to verify.
    c. Reassign messaging system users of the current main server to the messaging system used by the new main server. Enter test messages to verify.
13. Reboot the survivable remote server.
    a. Open a SAT session and enter `reset system 4`.

b. After the reboot, the survivable remote server should be registered with the main server and in a few minutes translations should be synchronized.

# Chapter 8: Conversion of IP-PNC port networks from simplex control to duplicated control

### About this task

This chapter describes the procedures to convert one or more IP-PNC port networks (PNs) from a simplex control configuration to a duplicated control configuration. The PNs are controlled by Duplex servers. For Communication Manager 6.2, the S8800, HP DL360 G7, and Dell R610 servers can be configured as Duplex servers.

**Note:**

This conversion adds a second TN2312BP IPSI circuit pack to an IP-PNC port network and a second Ethernet switch, if necessary, for connections between the servers and the IPSIs.

If the PN consists of G650 Media Gateways, the TN775 Maintenance circuit pack is not used, and, therefore, there is no cabling to a TN775 circuit pack.

## Converting IP-PNC port networks from simplex control to duplicated control

### Before you begin

Before you go to the customer site:

- Perform all the tasks mentioned in Presite checklist on page 15.
- Perform all the tasks mentioned in Performing preconversion tasks on page 20.
- Upgrade the system to Communication Manager release 6.2.

### About this task

To convert an IP-PNC port network from a simplex control network to a duplicated control network, perform the following tasks:

### Procedure

1. Install and cable a second Ethernet switch, if necessary. See *Installing and cabling a second Ethernet switch*.

2. Configure the SNMP subagent in the Avaya Ethernet switch, if used. See *Configuring the SNMP subagent in the Avaya Ethernet switch*.
3. Enable firewall settings, if necessary. See *Enabling firewall settings*.
4. Access the System Management Interface. See *Accessing the System Management Interface*.
5. Designate the slot for the duplicated IPSI circuit pack. See *Designating the slot for the duplicated IPSI circuit pack*.
6. Install the duplicated IPSI circuit pack. See *Installing the duplicated IPSI circuit pack*.
7. Add control network cabling for the new circuit pack. See *Adding control network cabling for the new circuit pack*.
8. Verify the IPSI circuit packs are inserted properly. See *Verifying insertion of IPSI circuit packs*.
9. Program the duplicated IPSI circuit pack. See Programming the duplicated IPSI circuit pack
10. Start a SAT session. See *Starting a SAT session*.
11. Administer the duplicated IPSI circuit pack on the server. See *Administering the duplicated IPSI circuit pack on the server*.
12. Verify IPSI translations. See *Verifying IPSI translations*.
13. Upgrade IPSI firmware, if necessary. See *Upgrading IPSI firmware*.

# Installing and cabling a second Ethernet switch

### About this task

### Procedure

To install and cable a second Ethernet switch, perform the following steps:

### Procedure

1. Install a second Ethernet switch, if necessary.

   This switch provides IP connections between the duplex servers and the duplicated TN2312BP IPSI circuit packs.
2. Ensure that a second or alternate Ethernet switch is already available if the customer has designated it.

However, if the control networks are dedicated (that is, not using the customer LAN for the server-to-IPSI connection), then a second Ethernet switch, from either Avaya or a third party, is required.

# Performing preconfiguration of the SNMP subagent in the Avaya Ethernet switch

### About this task

### Procedure

You must perform the following points before SNMP configuration.

### Procedure

1. Ensure that you are not using these procedures to set traps on a non-Avaya-provided Ethernet switch. These instruction apply only if using a new, Avaya-supplied Avaya Ethernet switch.
2. Refer to the documentation that comes with the Avaya Ethernet switch. The specific Avaya Ethernet switch model and firmware load shipped with a communication system may change over time. Therefore, this document is not specific on how to configure the SNMP subagent.
3. If the control network is non-dedicated (going over the customer's network), ensure that the 162/udp port for input to server is enabled (the default is disabled). Otherwise, the traps from the UPS(s) cannot be received. See Enabling firewall settings on page 60.
4. Administer the Simple Network Management Protocol (SNMP) subagent in the Avaya Ethernet switch so that it can report alarms to the server when the hardware experiences problems.
5. Each Avaya Ethernet switch requires a unique IP address, which can be a customer-provided one or the Avaya-provided default one. At a minimum, configure the following items:
   - IP address (1 for each Ethernet switch)
   - Subnet mask
   - Trap receiver IP address
   - Community string (get, set, trap)
     - Spanning tree version
     - Ethernet port speed (if applicable)
6. For the Ethernet switch to properly report alarms, configure the IP address(es) for the Ethernet switch(es).

7. See the Basic Configuration section of the Quick Start Guide and the documentation CD that comes with the Ethernet switch for the default user ID, password, and configuration commands.

## Configuring the SNMP subagent in the Avaya Ethernet switch

### Before you begin

You must read Performing preconfiguration of the SNMP subagent in the Avaya Ethernet switch on page 57.

### About this task

To administer the Ethernet switch:

### Procedure

1. Plug the Ethernet switch power cord into the back of the switch and the back of an UPS.
   - For a single control network, connect Ethernet switch 1 for Control Network A (CNA) into UPS 1.
   - For a duplicated control network, connect Ethernet switch 1 for CNA into UPS 1 and connect Ethernet switch 2 for Control Network B (CNB) into UPS 2.
2. Connect the services laptop computer (RS-232 serial port) to the port labeled Console on the front of Ethernet switch 1 (CNA) with the flat cable supplied with the Avaya Ethernet switch.
3. On the services laptop open a VT-100 terminal emulation session.
4. Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
5. Follow the instructions in the Quick Start Guide.
6. Set the following parameters:
   - IP address and subnet mask of the Ethernet switches:
     - For Ethernet switch for CNA, the defaults are 198.152.254.240, 255.255.0.0.
     - For Ethernet switch for CNB, the defaults are 198.152.255.240, 255.255.0.0.

- IP address of the trap receiver. (Do not use the Active Server IP address.)
  - For Ethernet switch for CNA, this is the IP address of server 1. (default is 198.152.254.200)
  - For Ethernet switch for CNB, this is the IP address of server 2. (default is 198.152.255.200)
- SNMP community string for Get, Set, and Trap. See the section on SNMP commands on the documentation CD that comes with the Avaya Ethernet switch.

**Security alert:**

The **Get** and **Set**, community name strings are generally configured with default values of Public and Private, respectively. These community name strings function as passwords for their respective SNMP operation. Avaya recommends changing these community name strings to something other than the default values. If a Network Management Station (NMS) is in operation on the network, whatever these strings are changed to must be communicated to the NMS administrator. If the defaults are left administered this could create a serious security issue. For example, the default Set community name string, with its widely known value of Private, could be used to reconfigure the Ethernet switch via SNMP message.

7. Verify that spanning tree is enabled (the default setting). Use the command **`set spantree enabled`**.
8. Set spanning tree version to rapid-spanning-tree (not the default). This command is available on Avaya P363 Ethernet switches having firmware version 4.0 or later. You must update the firmware to this version to use the command. Use the command **`set spantree version rapid-spanning-tree`**.

   **Note:**

   For more information on the Spanning Tree CLI commands, see *Installation and Configuration Guide, Avaya C360* and *Reference Guide, Avaya C360*, available at the Avaya Support website (http://www.avaya.com/support).
9. If IP-PNC, make sure all appropriate ports on the Ethernet switch are locked to 100 speed with full duplex.
10. When completed, disconnect the services laptop computer from the Ethernet switch.
11. If two Ethernet switches are present for CNA, repeat steps 1 through 7 for the second switch.
12. If a duplicated control network, repeat steps 1 through 9 for the remaining Ethernet switch(es).

# Enabling firewall settings

### Before you begin

For the server to receive SNMP traps from the UPS and Avaya Ethernet switch, you must enable the snmp trap, 162/udp port. The default is disabled.

### About this task

To enable firewall settings, perform the following steps:

### Procedure

1. Under Security, click **Firewall**.
2. Click **Advanced Settings. . .** to view the second page.
3. Scroll down until you see snmp trap, port 162/udp.
4. Select the box in the **Input to Server** column (far left) next to it.

# Accessing Communication Manager System Management Interface

### Procedure

1. Start the Web browser.
2. In the **Address** field, type `192.11.13.6` and press **Enter** to open the login Web page.
3. Log in as craft or dadmin.
4. Click **yes** to suppress alarms.

   The system displays the Communication Manager System Management Interface (SMI).

# Designating the slot for the duplicated IPSI circuit pack

### About this task

To designate the slot for the duplicated IPSI circuit pack, perform the following steps:

### Procedure

1. Designate the slot in which each new IPSI is to be installed.

Each of these circuit packs requires an I/O adapter that is installed on the backplane connector associated with the slot in which the circuit pack is installed.

2. Place the IPSI circuit packs in the slots specified in the Secondary, if duplicated control column in the table on page 61.

**Table 1: IPSI slot locations**

| Carrier/Gateway | Slot Number | |
|---|---|---|
| | Primary | Secondary, if duplicated control |
| G650 stack | A01 | B01 |
| SCC1 EPN | A00 | B01 |
| MCC1 EPN -- 1 PN | - Tone Clock slot (A00) | B01 |
| MCC1 EPN -- 2 PNs | - Tone Clock slot (A00)<br>- E02 | B01<br>D01 |
| MCC1 EPN -- 3 PNs | - Tone Clock slot (A00)<br>- B02<br>- D02 (single control)<br>- E02 (duplicated control) | Control duplication not supported with 3 PNs.<br>D01 (duplicated control) |
| MCC1 EPN -- 4 PNs | - Tone Clock slot (A00)<br>- B02<br>- C02<br>- D02 (single control)<br>- E02 duplicated control) | Control duplication not supported with 4 PNs<br>D01 (duplicated control) |
| MCC1 EPN -- 5 PNs | - Tone Clock slot (A00)<br>- B02<br>- C02<br>- D02<br>- E02 | Control duplication not supported with 5 PNs |

# Duplicated IPSI circuit pack Installation

You can Install the duplicated TN2312BP IPSI circuit pack for the following gateways:

- G650 Media Gateway
- MCC1 Gateway
- SCC1 Gateway

The installation procedure varies with the type of gateway you have selected for installation. You can insert the IPSI circuit pack and administer it ahead of time. The circuit pack is hot-swappable. Therefore, you do not need to turn off the PNs or the carriers.

For installation process, see Installing Duplicated IPSI circuit pack for G650 Media Gateway, for MCC1 Gateway, and for SCC1 Gateway.

## Installing Duplicated IPSI circuit pack for G650 Media Gateway

### Before you begin

Ensure that you have installed the IPSI in the appropriate slot number identified in the Secondary column on the right of ISPI Slot Locations table.

### About this task

To install the Duplicated IPSI circuit pack for G650 Media Gateway:

### Procedure

Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs into the B01 slot in gateway B.

## Installing Duplicated IPSI circuit pack for MCC1 Gateway

### Before you begin

Ensure that you have:

- Installed the IPSI in the appropriate slot number identified in the Secondary column on the right of ISPI Slot Locations table
- A short ribbon cable (comcode 700168727)

### About this task

To install the Duplicated IPSI circuit pack for MCC1 Gateway:

### Procedure

1. Insert the TN2312BP IPSI circuit pack part way into the TONE-CLOCK slot on the standby carrier (B).
2. Attach one end of the long ribbon cable to the connector on the component side of the circuit pack. The red line must be on the bottom (pin 1).
3. Push the tabs on the ends of the connector inward to lock the connector in place. See Ribbon Cable Connector.
4. Thread the ribbon through the slot on the front panel.

5. Attach the other end of the long ribbon cable to the bottom connector (labeled “B”) on the component side of the TN775D Maintenance (EPN) circuit pack. The red line must be on the bottom. See *High/Critical Reliability Ribbon Cable Connection*.
6. Fully insert the IPSI circuit pack.
7. Program the IPSI just inserted. See *Programming the duplicated IPSI circuit pack*.
8. Fully insert the TN775D Maintenance (EPN) circuit pack after the IPSI has been programmed.

## Installing Duplicated IPSI circuit pack for SCC1 Gateway

### Before you begin

Ensure that you have:

- Installed the IPSI in the appropriate slot number identified in the Secondary column on the right of ISPI Slot Locations table
- A long ribbon cable and the Cable PassThrough Kit (comcode 700219413)

### About this task

To install the Duplicated IPSI circuit pack for SCC1 Gateway:

### Procedure

1. Remove the ground plate, upper and lower rear covers from the gateways. See Removing ground plate and upper and lower rear covers..
2. Remove the TN2182 Tone Clock circuit pack from the new standby carrier (B). Place the circuit pack in an antistatic carrier.
3. Use the pass through tool to feed the long ribbon cable through gateway A. See Placing ribbon cable using the pass through tool.
4. Plug the long ribbon cable into the bottom connector (labeled B) on the component side of the TN775D Maintenance (EPN) circuit pack. The red line is on bottom. See *High/Critical ribbon cable connection*.
5. Thread the ribbon cable through the remaining slot on the faceplate of the TN775D Maintenance (EPN) circuit pack.
6. Route the cable through the TDM slot in the back of the SCC1 gateway A and up to SCC1 gateway B. See *Cable routing through the TDM slot*.
7. Use the pass through tool to feed the long ribbon cable through gateway B.
8. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs part way into its designated slot in gateway B.

9. Connect the long ribbon cable to the connector on the component side of the TN2312BP Internet Protocol Server Interface (IPSI) in gateway A (red line on bottom). See *High/Critical ribbon cable connection*.
10. Fully insert the TN775D Maintenance (EPN) and TN2312BP Internet Protocol Server Interface (IPSI) circuit packs.
11. If both ribbon and CAT5 cables were installed, replace rear covers and ground plates. See *Replacing rear covers and ground plates*. If CAT5 cables need to be installed, leave the rear covers and ground plates off and see *Adding control network cabling for the new circuit pack*.

## Ribbon Cable Connector

The following image explains Ribbon Cable Connector.

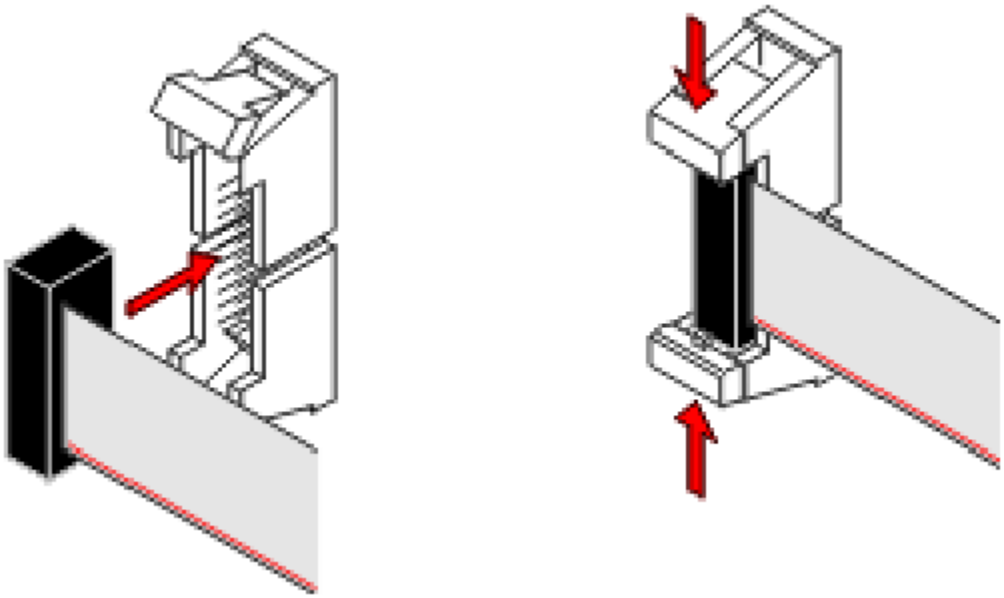

**Figure 1: Ribbon Cable Connector**

## High/Critical Reliability Ribbon Cable Connection

The following image explains High/Critical Reliability Ribbon Cable Connection.

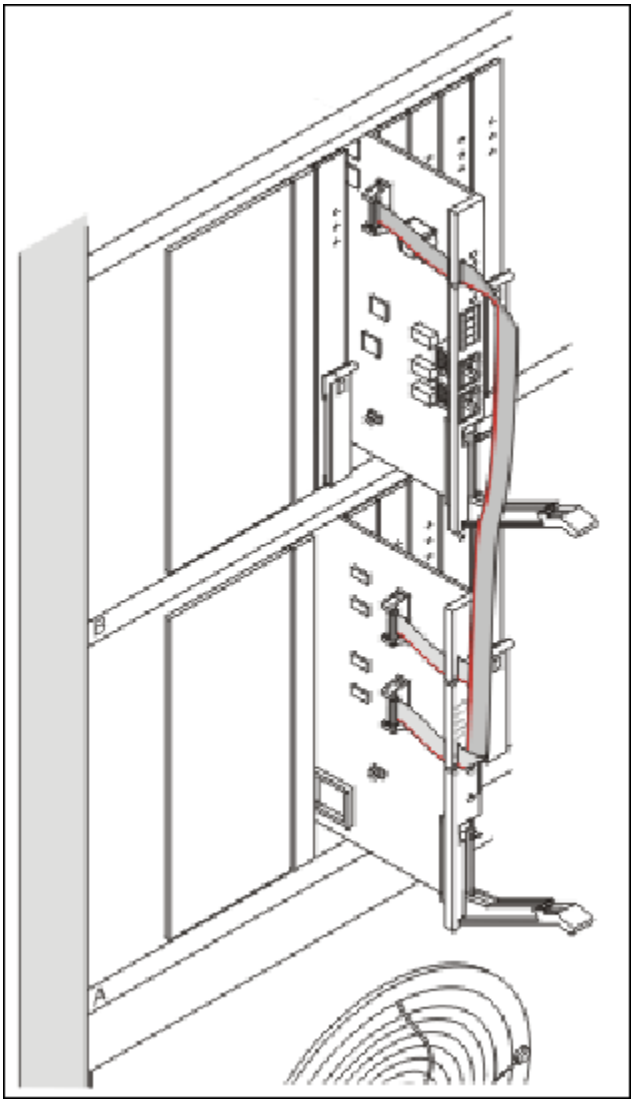


**Figure 2: High/Critical Reliability Ribbon Cable Connection**

## Removing ground plate and upper and lower rear covers

### About this task

The following image explains the process of removing ground plate and upper and lower rear covers.

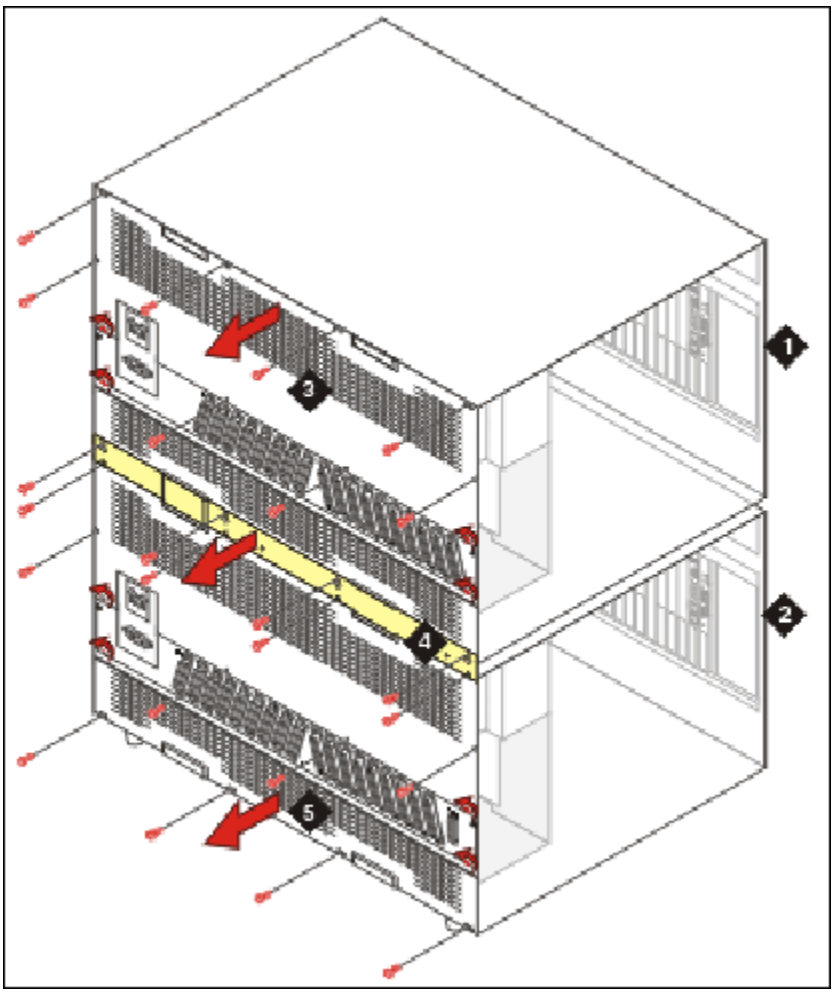


**Figure 3: Removing ground plate and upper and lower rear covers (SCC1 shown)**

| Number | Description |
|---|---|
| 1 | Gateway B |
| 2 | Gateway A |
| 3 | Upper rear cover |
| 4 | Ground plate |
| 5 | Lower rear cover |

# Placing ribbon cable using the pass through tool

## About this task

The following image explains the process of placing ribbon cable using the pass through tool.

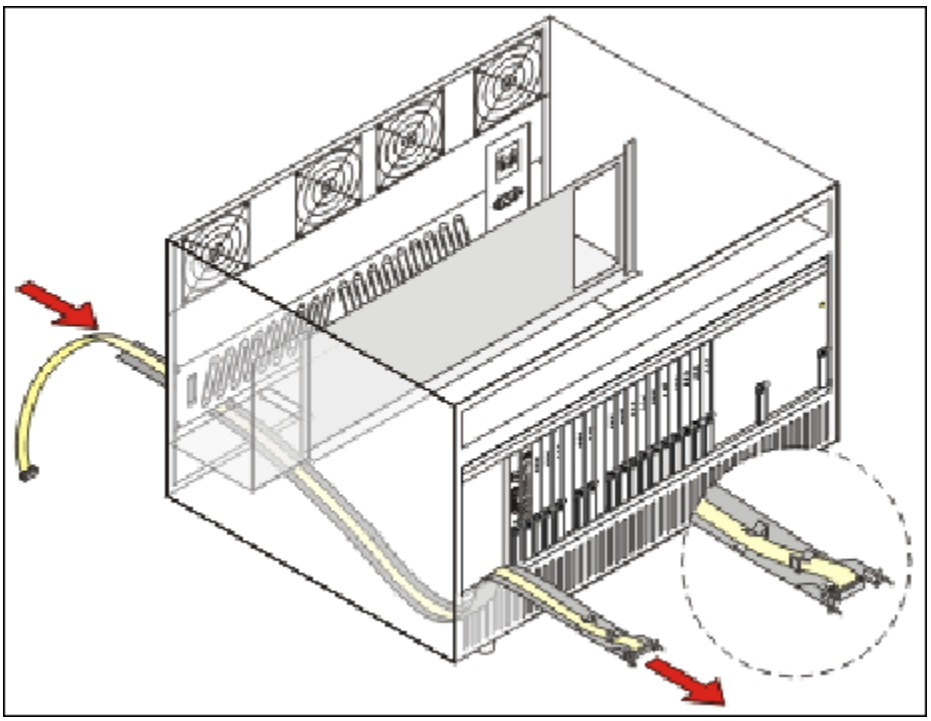

**Figure 4: Ribbon cable placement using the pass through tool**

## Connecting High/Critical Ribbon Cable

### About this task

The following image explains the process of High/Critical ribbon cable connection.

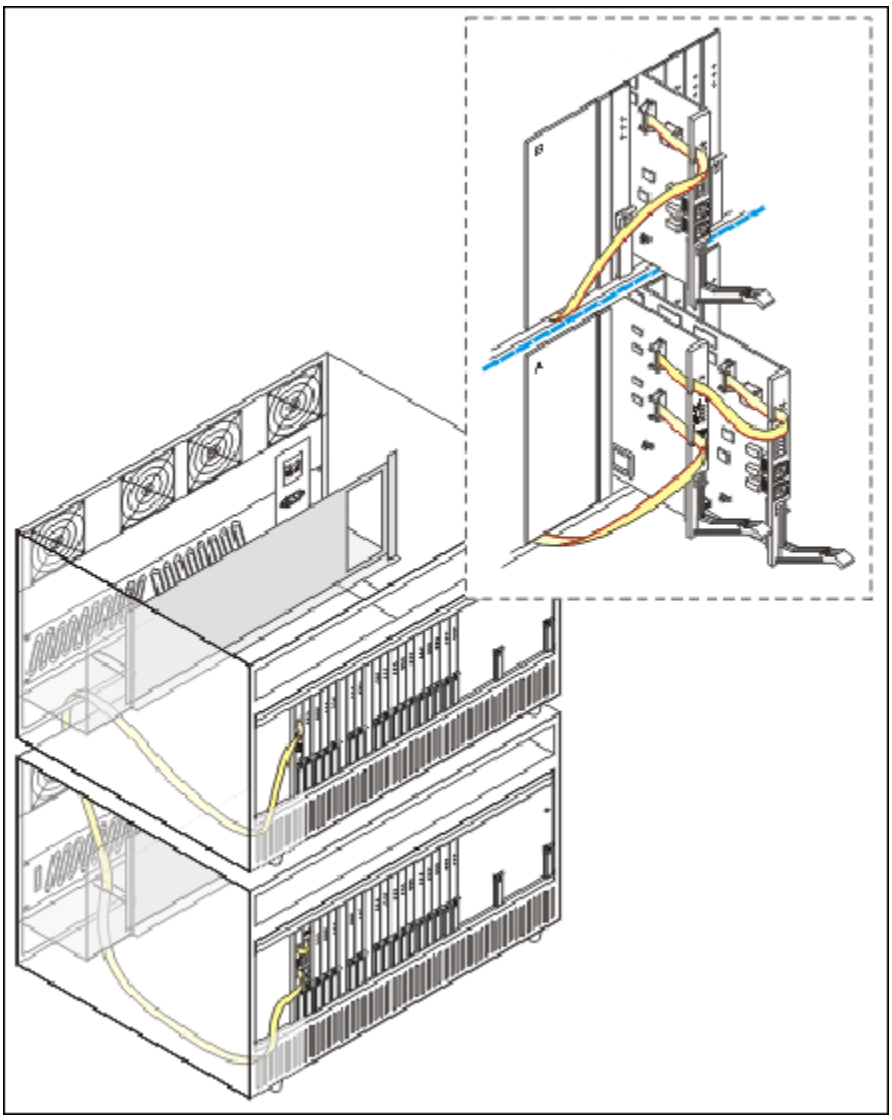

**Figure 5: High/Critical Ribbon Cable Connection**

## Routing a Cable through the TDM slot

### About this task

The following image explains the process of cable routing through the TDM slot.

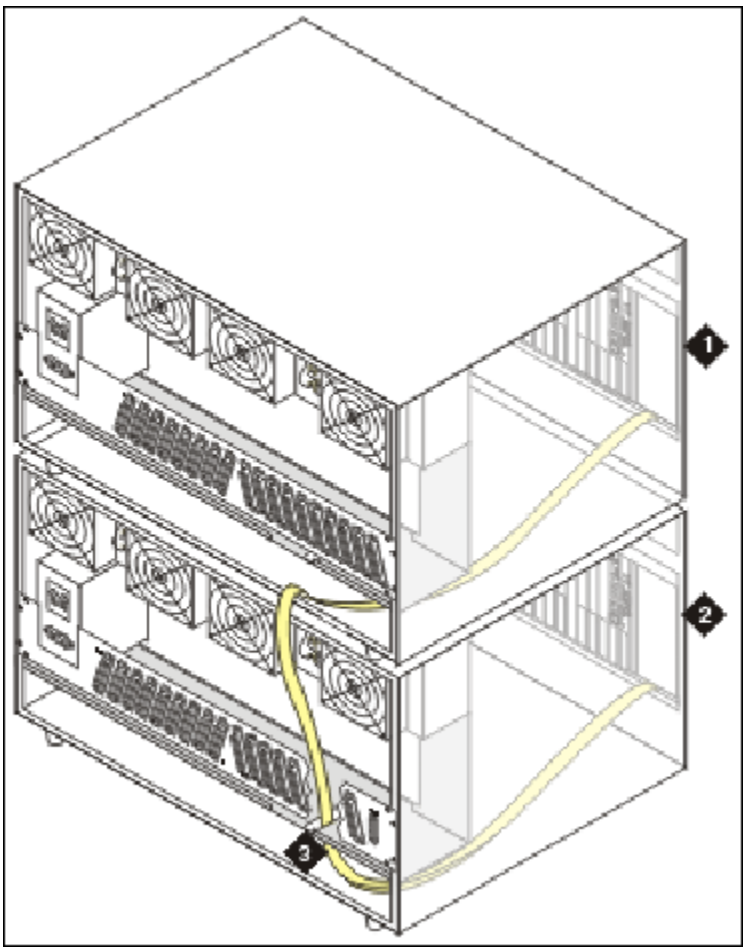


**Figure 6: Cable routing through the TDM slot**

| Number | Description |
|---|---|
| 1 | Gateway B |
| 2 | Gateway A |
| 3 | TDM cable slot |

## Replacing rear covers and ground plates

### About this task

The following image explains the process of replacing rear covers and ground plates.

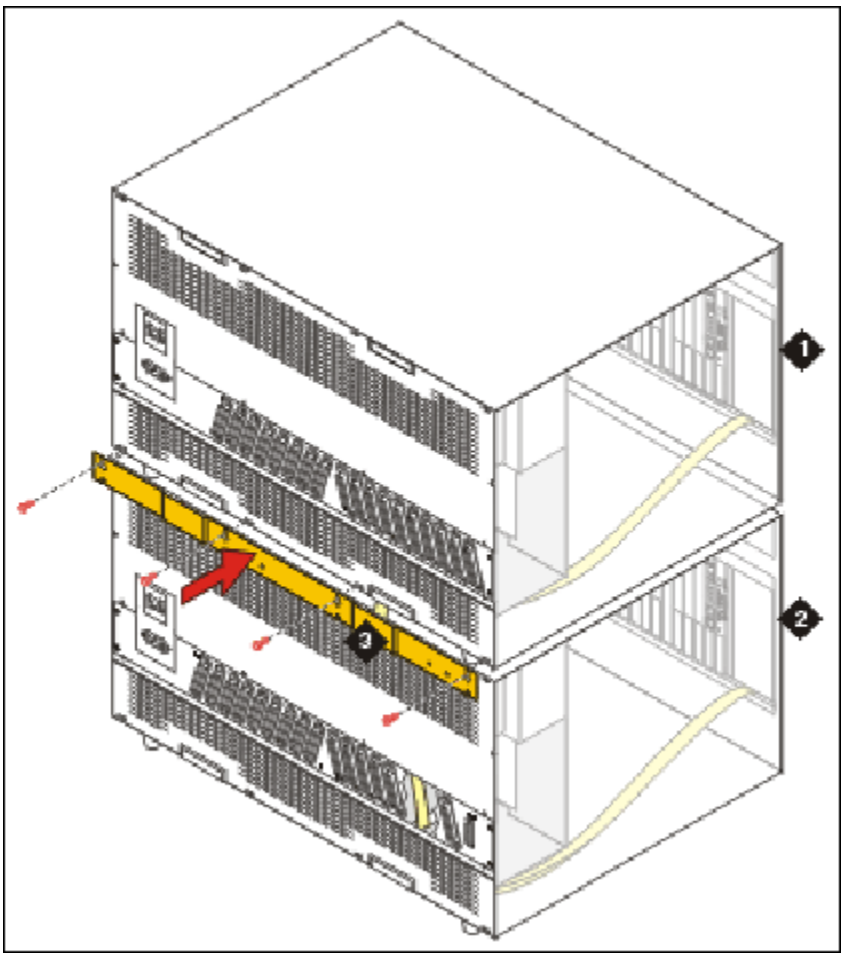


**Figure 7: Rear covers and ground plates replacement (SCC1 shown)**

| Part | Description |
|---|---|
| 1 | Gateway B |
| 2 | Gateway A |
| 3 | Ground plate covering TDM cable opening. Note: All cables running between or exiting gateways use the opening provided for TDM cables. |

# Adding control network cabling for the new circuit pack

## About this task

To connect the duplicated IPSI slot to the control network:

### Procedure

1. Connect the TN2312BP I/O Adapter to the backplane amphenol connector that corresponds to the slot in which the TN2312BP is installed.
2. Connect a CAT5 or better Ethernet cable to the RJ45 connector on the IPSI adapter.
3. Connect the other end of the CAT5 cable to the new, or alternate, Ethernet switch.

# Verifying the IPSI circuit packs are inserted properly

### About this task

To check that the IPSI circuit packs are inserted properly,

### Procedure

1. Enter `display circuit-pack` *cabinet number* to open the SAT Circuit Packs window, after one minute.
2. Verify that the TN2312B circuit packs are shown in the appropriate slots.

# Programming the duplicated IPSI circuit pack

### About this task

For programming the duplicated IPSI circuit pack, perform one of the following two steps for static addressing.

### Procedure

1. For Static addressing with non-dedicated control networks, clear the ARP cache on the laptop before connecting to another IPSI by entering `arp -d 192.11.13.6` at the Windows command prompt.
2. For static addressing instead of DHCP, perform the following steps:
   a. Connect the services laptop to the Services port on the IPSI faceplate.
   b. Enter `telnet 192.11.13.6` to telnet to the IPSI.
   c. At the IPSI prompt, enter `ipsilogin` to log in to the IPSI IP Admin Utility.
   d. Log in with craft and the IPSI password.

e. Enter `set control interface` *ipaddr netmask* to enter the static IP address and netmask.
f. Enter `quit` to save the changes and exit the IPSI session.
g. Telnet to 192.11.13.6 and login.
h. Enter `show control interface`.

   The system displays the IP address, subnet mask, and default gateway information.
i. Verify that the proper information was entered.

   - If a default gateway is used, enter `set control gateway` *gatewayaddr* where *gatewayaddr* is the customer-provided IP address for their gateway.
   - Enter `quit` to save the changes and exit the IPSI session.
   - Telnet to 192.11.13.6 and login.
   - Use **`show control interface`** to verify the administration.
   - Enter `quit`. Then enter `reset` and answer y (yes).
j. Set VLAN and diffserv parameters, if required. See *Setting VLAN and diffserv parameters*.

## Setting VLAN and diffserv parameters

### Procedure

1. Log back in to the new IPSI.
2. Enter `show qos` to display the quality of service values.
3. If necessary, 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.

   - Enter `set vlan priority 6`
   - Enter `set diffserv 46`
   - Enter `set vlan tag on`
   - Enter `set port negotiation` *1 disable*
   - Enter `set port` *duplex 1 full*
   - Enter `set port speed` *1 100*

4. Enter `show qos` to check the administered values.
5. Enter `quit` to exit.

   **Important:**

   Ensure that the port settings on the Ethernet switches are set to the same values as in the **`set port`** commands.
6. Telnet to the IPSI and log in.
7. Enter `reset`.

   Enter `y` in response to the warning.
8. Disconnect the laptop from the IPSI.
9. Verify that the LED display on the IPSI faceplate contains I P and a filled-in V at the bottom.

# Starting a SAT session

### Procedure

1. Open a terminal emulation application, such as MS HyperTerminal.
2. Type `192.11.13.6 5023` and press **Enter**.
3. Log on as craft or dadmin.
4. Supress alarm origination.

# Administering the duplicated IPSI circuit pack on the server

### About this task

To administer the TN2312BP circuit pack on the server, perform the following steps:

### Procedure

1. On the SAT command line interface, enter `change system-parameters duplication` and set **Enable Operation of IPSI Duplication** to y.

   Step 1 needs to be completed just once for all IPSIs.

2. Enter `add ipserver-interface` *n*, where *n* is the PN number to add the new IPSI.

   Step 2 must be repeated for each duplicated IPSI you are adding.

# Verifying IPSI translations

### Procedure

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

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a *1* shows in any position, you must troubleshoot the problem.

   **Note:**

   The pattern 0.1.1.0 usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

# Upgrading IPSI firmware

### About this task

To upgrade firmware on the IPSIs, perform the following steps:

### Procedure

1. For Prerelease 5.2 use the Maintenance Web Interface.
2. Copy IPSI firmware to the media processor hard drive. Use **Download Files** under **Miscellaneous**.
3. Determine which IPSIs you need to upgrade, with **IPSI Version** under **IPSI Firmware Upgrades**.
4. Download the new firmware to the IPSIs. Use **Download IPSI Firmware**.
5. Use **Activate IPSI Upgrade** to activate the new firmware.
6. When the IPSIs are recovered, use **IPSI Version** to verify the firmware versions.

For more information about upgrading the IPSI firmware, see *Upgrading Avaya Aura® Communication Manager, 03-603560*.

# Chapter 9: Conversion of IP-PNC port networks from simplex bearer to duplicated bearer

This chapter describes the procedures to convert an Internet Protocol port network connectivity (IP-PNC) configuration from simplex bearer reliability to duplicated bearer reliability. The port networks (PNs) are controlled by duplex servers. All voice and data transmission between the PN you are converting and other PNs in the network occurs over the LAN/WAN of the customer.

If the active media processor, or connections to it, fail, active connections failover to the standby media processor and remain active. This duplication prevents calls from being dropped in case of failure.

**Note:**

Only two TN2602AP circuit packs are allowed per PN.

**Caution:**

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

## Duplicated control network

Avaya strongly recommends a duplicated control network be configured prior to or along with the conversion to duplicated bearer. Though existing connections may continue during most failures to the PN, no new connections can be made if the control network is part of the failure.

## Overflow with coresident TN2302AP circuit packs

If you anticipate that at peak traffic periods, traffic on the PN will exceed the maximum administered VoIP channels, 80 or 320, of the TN2602AP circuit pack, a TN2302 may be coresident. Communication Manager will pass excess traffic over the TN2302 at peak traffic periods, but these calls will not be supported by the duplicated reliability.

# Reduced channels with duplicated TN2602AP circuit packs

If a pair of TN2602AP circuit packs previously used for load balancing are readministered 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 80 voice channels, and you readminister the circuit packs to be in bearer duplication mode, you will have 80 (not 160) channels available.
- If you have two TN2602 AP circuit packs in a load balancing configuration, each with 320 voice channels, and you readminister the circuit packs to be in bearer duplication mode, you will have 320 (not 484 — see the note that follows) channels available.

**Note:**

When two TN2602AP circuit packs, each with 320 voice channels, are used for load balancing within a PN, the total number of voice channels available is 484, not 640, because 484 is the maximum number of time slots available for connections within a PN.

# Performing preconversion tasks to convert IP-PNC port networks from simplex to duplicated bearer

### About this task

Before you start conversion, you must be aware of the following information:

### Procedure

1. Ensure that there are no fiber links to other PNs.

   If there are fibre links, convert the PN from fiber-PNC to IP-PNC. If necessary, see **Converting from fiber port networks to IP-PNC** in *Upgrading to Avaya Aura® Communication Manager, 03-603560*.

2. Ensure that you have the most recent firmware for duplicated TN2602AP circuit packs.

   If you do not have the most recent and appropriate firmware, upgrade the firmware on the circuit packs.

**Note:**

Non-duplicated TN2602AP firmware is different from duplicated TN2602AP firmware. Be sure the firmware you have is for duplicated TN2602AP circuit packs.

3. Install a TN771DP maintenance test circuit pack in each IP-PNC PN that has both duplicated control and duplicated bearer.
4. Perform all the tasks mentioned in Presite checklist on page 15.
5. Unless one of the following conditions exists, ensure that you have IP addresses, node names, and slots for the TN2602AP IP Media Resource 320 circuit packs:
   - You are replacing TN2302 circuit packs with the TN2602AP circuit packs and therefore are not reusing the TN2302 IP addresses, node names, and slots.
   - You are reusing load-balanced TN2602AP circuit packs that are already installed in the PN.
6. Ensure that you have the subnet mask and the default gateway IP address.

   **Note:**

   Get this information from the project manager or the network administrator of the customer.
7. Ensure that the Communication Manager license file have at least two entries, either VALUE_2602_80VC or VALUE_2602_320VC, with the same number of VoIP channels - either both 80 or both 320.
8. **(Optional)** Install a second Ethernet switch, if necessary, for connections to the network for the duplicated TN2602AP circuit packs. Adding a second Ethernet switch adds reliability to the duplicated bearer network. That is, if the failure is at the Ethernet switch or its connection to the TN2602AP circuit pack, the standby TN2602AP circuit pack can handle traffic through the alternate Ethernet switch.

   If there are already two Ethernet switches for duplicated control and the Ethernet switches are also connected to the customer LAN, you do not need a second Ethernet switch.
9. **(Optional)** Install a second UPS to support the second Ethernet switch, if you have installed a second Ethernet switch.

   **Caution:**

   If, in the unlikely event that a failure occurs on an active TN2602AP circuit pack during the setup and administration of duplication, active calls being carried on the circuit pack are dropped. In addition, TN2602AP call processing and interchange activity is tracked through the MEDPRO-C maintenance object. See *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430, for more information.

# Converting IP-PNC port networks from simplex bearer to duplicated bearer

### About this task

This section describes the process for converting a port network to duplicated TN2602AP IP Media Resource 320 circuit packs.

For installation and conversion process, perform the following tasks:

### Procedure

1. Check your shipment, if not reusing existing TN2602AP circuit packs. See *Checking the shipment*.
2. Access the System Management Interface. See *Accessing the System Management Interface*.
3. Access the server command line interface with ssh protocol. See *Accessing the server command line interface with ssh protocol*.
4. Check software release. See *Checking software release*.
5. Determine the existence and location of TN2302 and TN2602AP circuit packs. See *Determining the existence and location of TN2302 and TN2602AP circuit packs*.
6. Upgrade firmware on the existing TN2602AP circuit packs, if necessary. See *Upgrading firmware on the existing TN2602AP circuit packs*.
7. Disable an existing TN2602AP circuit pack or TN2302 circuit packs. See *Disabling an existing TN2602AP circuit pack or TN2302 circuit packs*.
8. Remove the TN2302 circuit pack hardware. See *Removing the TN2302 circuit pack hardware*.
9. Connect the cables to any new TN2602AP circuit packs. See *Connecting the cables to any new TN2602AP circuit packs*.
10. Install the TN2602AP circuit packs, if new. See *Installing the TN2602AP circuit packs*.
11. Install the TN771DP Maintenance Test circuit pack. See *Installing the TN771DP Maintenance Test circuit pack*.
12. Verify installation and voice channels. See *Verifying installation and voice channels*.
13. Upgrade firmware on the new TN2602AP circuit packs, if necessary. See *Upgrading firmware on the new TN2602AP circuit packs*.
14. Administer the node name for the TN2602AP circuit pack, if necessary. See *Administering the node name for the TN2602AP circuit pack*.

15. Administer the IP interface for the TN2602AP circuit packs. See *Administering the IP interface for the TN2602AP circuit packs*.
16. Test the external connection to the LAN. See *Testing the external connection to the LAN*.
17. Verify active call status. See *Verifying active call status*.

# Checking the shipment

### Before you begin

Ensure that you have a list of required hardware and related items. See Required Hardware section.

### About this task

When the order arrives at your site, perform the following steps to check the contents:

### Procedure

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 for each TN2602AP IP Media Resource 320 circuit pack mentioned in Required Hardware section.
3. Read and follow any directions inserted into the package by the factory.

# Hardware components

The following is a list of hardware components:

- TN2602AP IP Media Resource 320 (MedPro) [Code: 108566381] [Required quantity: 1 or 2/PN]
- Media Resource 320 Adapter with retainer clip [Code: 700283690] [Required quantity: 1/MedRes]

  The adapter has an amphenol connector on one side, an RJ45 connector and 2 Ethernet ports on the other for connecting to the network. See Media Resource 320 Adapter.
- Migration kit (PEC code 63275) [Code: 700234032] [Required quantity: 1 or 2/PN]

You need Migration kit (PEC code 63275) only if installation is being performed in old carriers or cabinets with WP cables.

- Upper circuit pack slot label [Code: 700207111] [Required quantity: 1]
- Twisted pair I/O cables [Code: 700181118] [Required quantity: 10]

Only one cable is needed for each circuit pack.

- Beside the above mentioned items:
  - The customer must provide one CAT5 or better cable for each TN2602AP.
  - One TN771DP maintenance test circuit pack is required in an IP-PNC PN that has both duplicated control and duplicated bearer.

# Accessing Communication Manager System Management Interface

## Procedure

1. Start the Web browser.
2. In the **Address** field, type `192.11.13.6` and press **Enter** to open the login Web page.
3. Log in as craft or dadmin.
4. Click **yes** to suppress alarms.

   The system displays the Communication Manager System Management Interface (SMI).

# Accessing the server command line interface with ssh protocol

## About this task

- To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. In addition, a third-party ssh client must already be installed on your computer.
- PuTTY is one such client available for download from http://www.putty.nl/download.html. The following procedure describes, as an example of ssh access, how to log into the server command line with PuTTY.

**Note:**

A version of PuTTY that is defaulted for ssh server access is available for Avaya services personnel only. In this version, some values below have already been preselected.

**Caution:**

While a variety of Avaya products support access using ssh, Avaya does not provide support for third-party clients used for ssh access. Any problems with an ssh client, including PuTTY, are the responsibility of the user or the ssh client vendor.

To access the command line interface using PuTTY with ssh:

## Procedure

1. On your computer, click on the **PuTTY** desktop link or select **Start** > **Programs** > **PuTTY** > **PuTTY**.
2. In the **Host Name** (or **IP address**) field, type `192.11.13.6` if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.
3. In the **Port** field, type `22` (the SAT is 5022).
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection** > **SSH**.
   The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select 2.
7. In the Encryption options window, use the up and down arrows to set AES (SSH-2) as the top option and 3DES as the second option.

   **Note:**

   You can save the PuTTY settings and customize the PuTTY tool with other settings, such as for color. For documentation on PuTTY, see http://www.putty.nl/docs.html.
8. In the PuTTY menu on the left, click **Terminal** > **Keyboard**.
   The Options controlling the effects of keys dialog box opens.
9. In the Backspace key area, select **Control-H**.
   This activates the backspace key while you are using the SAT.
10. Click **Open**.

    **Note:**

    If you have not connected to this particular server before, ssh prompts you to accept the server host key. If you save this key when prompted, you will not be prompted if you connect again later. If you do not save the key, PuTTY prompts you the next time you connect to this server.

    When connecting through the Services laptop interface on the server, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as

192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.

11. If necessary, click **Yes** to accept the server's host key.
12. Log in to the server.

# Checking software release

### About this task

To verify the software version, perform the following steps:

### Procedure

1. Under Server, click **Software Version**.
2. Look in the **Reports as** field to verify that the new software is running correctly. If it is, see the next step.

# Determining the existence and location of TN2302 and TN2602AP circuit packs

### About this task

To determine the location of existing TN2302 IP Media Processor circuit packs, perform the following steps:

### Procedure

1. Enter `display circuit-packs` *port network #*, where *port network #* is the PN in which you are adding duplicated TN2602AP circuit packs.

   A list of circuit packs appears.
2. Locate and record the location of the TN2602AP circuit packs, if any.
3. If there is only one or no TN2602AP circuit packs, locate one or two TN2302 circuit packs for replacement with TN2602AP circuit packs.

   **Important:**

   Avaya recommends that you install duplicated TN2602AP circuit packs in different carriers or cabinets whenever possible. Doing so adds reliability in the event of carrier or cabinet failure.

4. Enter `display ip-interface` *UUCSS* for each of the TN2302 circuit packs you are replacing or the currently installed TN2602AP circuit packs, if any.
5. Record the existing administrative data.

**Note:**

You can use the same node names and IP addresses as those formerly used by the TN2302 circuit packs.

## Upgrading firmware on the existing TN2602AP circuit packs

### About this task

To upgrade the firmware on existing TN2602AP circuit packs, perform the following steps:

### Procedure

1. Enter `campon-busyout media-processor` *UUCSS*, where *UUCSS* is the location of a TN2602AP circuit pack you are converting.
2. Wait until all calls the circuit pack is carrying have ended.
3. Upgrade the firmware. (See *Upgrading Avaya Aura® Communication Manager, 03-603560*.)
4. When the firmware has been installed, enter `release board` *UUCSS*.
5. Repeat steps 1 through 4 for the other TN2602AP circuit pack, if it exists.

## Disabling an existing TN2602AP circuit pack or TN2302 circuit packs

### About this task

You have to disable the TN2302 or TN2602AP circuit packs to reuse their slots and to convert an existing TN2602AP circuit pack from a load-balancing circuit pack to a standby duplicated bearer circuit pack.

**Note:**

Disabling the TN2302 circuit packs is optional. However, all bearer traffic is handled by the active TN2602AP circuit pack unless all channels are busy. Any overflow traffic is then handled by any remaining TN2302 circuit packs.

To disable the TN2302 or TN2602AP circuit packs, if any, perform the following steps:

### Procedure

1. Enter `campon-busyout media-processor` *UUCSS*, where *UUCSS* is the location of a TN2302 circuit pack you are replacing or the TN2602AP you are converting.
2. Wait until all calls the circuit pack is carrying have ended.
3. Enter `change ip-interface` *UUCSS*, where *UUCSS* is the location of a TN2302 circuit pack you are replacing or the TN2602AP circuit pack you are converting.
4. Enter `n` in the **Enable Ethernet Port** field.
5. Enter `remove ip-interface` *UUCSS* to remove the TN2302 or TN2602AP circuit pack from Communication Manager software.
6. Repeat steps 1 through 5 for the additional TN2302 circuit packs you are removing.

## Removing the TN2302 circuit pack hardware

### About this task

To remove the TN2302 circuit pack hardware, perform the following steps:

### Procedure

1. Unseat the TN2302 circuit pack from its slot.
2. Disconnect the network cable(s) to the ETHERNET connector on the TN2302AP backplane adapter(s).
3. Disconnect the amphenol connector on the adapter from the amphenol connector corresponding to each TN2302AP slot.
4. Repeat steps 1 through 3 for the next TN2302 circuit pack.

## Connecting the cables to any new TN2602AP circuit packs

### Before you begin

You need to cable any new TN2602AP circuit packs you are installing in the port network.

### About this task

To install the cable for an IP Media Resource 320 circuit pack, perform the following steps:

**Note:**

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

**Important:**

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

### Procedure

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

## Media Resource 320 Adapter

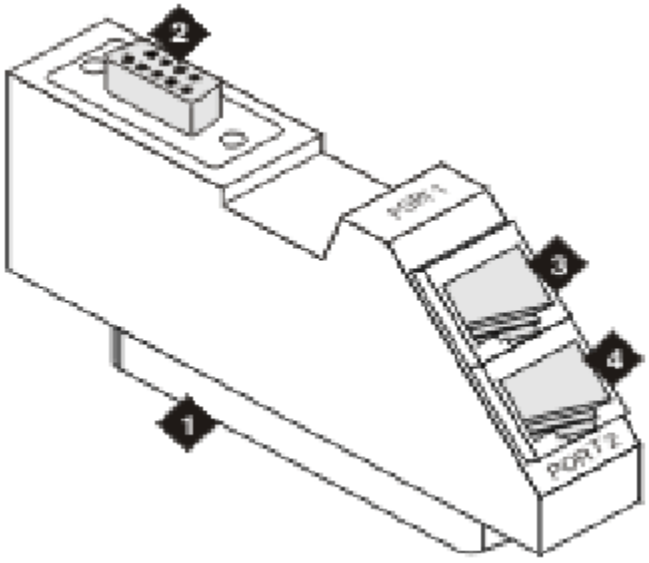


**Figure 8: Media Resource 320 Adapter**

| Number | Description |
|---|---|
| **1** | Amphenol connector to backplane connector corresponding to TN2602AP slot |
| **2** | RS-232 connector for services |
| **3** | Port 1: RJ45 LAN cable connection for 100 Mbps CAT5 cable |

| Number | Description |
|---|---|
| 4 | Port 2: RJ45 LAN connection for future use (do not use) |

# Installing the TN2602AP circuit packs

## Before you begin

**Caution:**

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

## About this task

**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 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.

## Procedure

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

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

# Installing the TN771DP Maintenance Test circuit pack

### Procedure

If the PN will have both duplicated control and duplicated bearer, install a TN771DP circuit pack.

# Verifying installation and voice channels

### About this task

**Note:**

If you are reusing two existing TN2602AP circuit packs, you can skip this task.

To verify the installation, perform the following steps:

### Procedure

1. Enter `list configuration board` *UUCSS*, where *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
2. Verify that TN2602AP shows in the slot location.
3. Look under the Vintage column and note the firmware version. If the firmware version is not the most recent available from the Avaya Downloads website, you must upgrade the firmware on the circuit pack.
4. Enter `display system-parameters customer-options`.
5. Go to page 2 of the Option Features window.

```
display system-parameters customer-options                      Page   2
of  11
                                OPTIONAL FEATURES
IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 425
          Maximum Concurrently Registered IP Stations: 18000 0
            Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
             Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 788
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
```

```
                    Maximum Media Gateway VAL Sources: 250   1
          Maximum TN2602 Boards with 80 VoIP Channels: 128   0
Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
        (NOTE: You must logoff & login to effect the permission changes.)
```

6. Find the appropriate field, either the **Maximum TN2602 Boards with 320 VoIP Channels** or **Maximum TN2602 Boards with 80 VoIP Channels** field. Subtract the number in the Used column with the maximum number listed to the left of the Used column.

   If you are installing two new TN2602AP circuit packs, there must be two circuit packs of the same number of channels available. If not, a new license must be installed. If you are installing one new TN2602AP because the PN already has one available, then there must be one circuit pack of the same number of channels available.

# Upgrade firmware on the new TN2602AP circuit packs

If you determined that you must upgrade the firmware on newly-installed TN2602AP circuit packs, see *Upgrading Avaya Aura® Communication Manager, 03-603560*.

# Administering the node name for the TN2602AP circuit pack

## About this task

**Note:**

If you are replacing one or two TN2302 circuit packs, you can reuse the node name and IP address for those circuit packs. Therefore, you may be able to skip this task for one or both TN2602AP circuit packs.

To administer the node names for the circuit packs, perform the following steps:

## Procedure

1. Enter `change node-names ip`.

```
change node-names ip                                        Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
BikCMprocr             10.13.11.22
clan                   10.13.11.113
clan2a02               10.13.15.92
clan2a06               10.13.15.96
default                0.0.0.0
gateway                10.13.1.1
```

```
lsp                 10.13.17.63
medpro              10.13.11.114
medpro2a08          10.13.15.95
procr               10.13.11.6
procr1.12           10.13.1.12
procr11.26          10.13.11.26
procr17.3           10.13.17.3
procr17.43          10.13.17.43
procr20.23          10.13.20.23
procr32.1.20        10.32.1.20
( 16 of 26   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-
name
```

2. Enter in the node names and IP addresses for the TN2602AP.
3. Enter `display circuit-packs`. Verify that the TN2602AP shows up in the Code column.
4. Repeat steps 1 through 3 for the second circuit pack, if necessary.

# Administering the IP interface for the TN2602AP circuit packs

### About this task

To administer the IP interface for the circuit packs, perform the following steps on the circuit pack you want to be the active circuit pack:

**Note:**

Any calls active when you start this procedure continue to use the physical IP address of the TN2602AP circuit pack for the connection, not the virtual IP address you are setting in this procedure. Therefore, any of these calls, if they continue after you complete this procedure, will drop in the event of an interchange.

### Procedure

1. Type one of the following commands:
   - For a previously-existing TN2602AP circuit pack that is still administered, enter `change ip-interface` *UUCSS*, where *UUCSS* is the cabinet, carrier, and slot location.
   - For a newly-installed TN2602AP circuit pack that you are administering as the active circuit pack, enter `add ip-interface` *UUCSS*.

```
add ip-interface 1a03                                        Page 1 of 1
                                    IP INTERFACES
                                Critical Reliable Bearer? n
                    Type: MEDPRO
```

```
                  Slot: 01A03
            Code/Suffix: TN2602
              Node Name: medres03a01
             IP Address: 192.168.1.82
            Subnet Mask: 255.255.255.0
        Gateway Address: . . .
   Enable Ethernet Port? y
         Network Region: 1
                   VLAN: n
                                ETHERNET OPTIONS
                  Auto? n
                 Speed: 100 Mbps
                Duplex: Full
```

2. In the **Critical Reliable Bearer?** field, enter `y`.

   A second column of data for a standby TN2602AP appears on the right of the window.

```
add ip-interface 1a03                                          Page 1 of 1
                                  IP INTERFACES
                            Critical Reliable Bearer? y
                    Type: MEDPRO
                    Slot: 01A03                          Slot:
              Code/Suffix: TN2602                  Code/Suffix:
                Node Name: medpro03a01               Node Name:
               IP Address: 192.168.1.82             IP Address:
              Subnet Mask: 255.255.255.0
          Gateway Address: . . .
     Enable Ethernet Port? y              Enable Ethernet Port? y
           Network Region: 1
                    VLAN: n                              VLAN: n
            VOIP Channels: xxx
  Shared Virtual Address: 255.255.255.255
       Virtual MAC Table:                 Virtual MAC Address:
                                    ETHERNET OPTIONS
                    Auto? n                              Auto? n
                   Speed: 100 Mbps                      Speed: 100 Mbps
                  Duplex: Full                         Duplex: Full
```

3. Complete the following fields.
   - The **Type**, **Slot**, **IP Address**, and **Code/Suffix** fields for the active circuit pack are populated automatically.
   - In the **Node Name** field, enter the same node name entered on the Node Name window.
   - 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 80 or 320, depending on the number of circuit packs that are licensed for each, and the capacity the customer needs for this PN. This setting also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is y.
- 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 PN under the control of a different Communication Manager main server has duplicated TN2602AP circuit packs.
  - That PN controlled by a different main server has the same number as the PN in which you are administering the TN2602AP circuit packs.
  - The PN or its main server connects to the same Ethernet switch as the PN in which you are administering the TN2602AP circuit packs.

  Selecting a different Virtual MAC Table from that chosen for a PN that has the previously-listed conditions helps prevent the possibility that two TN2602AP circuit packs within the customer network will have the same virtual MAC address.
- The **Virtual MAC Address** field is populated automatically with a MAC address from the Virtual MAC Table you select.

4. Complete the following fields for the standby TN2602AP circuit pack:
   - In the **Slot** field, type the slot number of TN2602AP circuit pack.
   - In the **Node name** field, type the name of the TN2602AP circuit pack.
   - Set the **Enable Ethernet Port** field to y.
   - Set **VLAN** to n.
   - Set Ethernet Options to match the customers network for both circuit packs. The recommended settings are
     - **Auto** n (default)

   If you enter `n`, also complete the following fields. The recommended values display.
   - **Speed**: 100 Mbps
   - **Duplex**: Full
5. Press **Enter** to save the information and effect the new settings.

# Testing the external connection to the LAN

### About this task

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 window reads `pass`. If it reads `abort`, verify the IP-address information and check the connectivity, including the cabling.

### Procedure

1. Enter `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.

   ```
   ping ip-address 192.168.10.38 board 02B05
                              PING RESULTS
     End-pt IP         Port      Port Type  Result    Time(ms)  Error Code
     192.168.10.21     01A13      MEDRES    PASS       10
   ```

2. If step 1 passes, enter `ping ip-address` *ipaddress* `board` *UUCSS*, where *ipaddress* is the IP address of an endpoint on the gateway of the customer and *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP circuit pack you are testing.
3. If step 2 passes, enter `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.

### Result

The TN2602AP IP Media Resource 320 circuit pack is now installed in the gateway and connected to the IP network.

# Verifying active call status

### About this task

To verify that calls are being processed:

### Procedure

1. Make an external trunk call to a telephone on the PN and leave the call active.

2. Enter `status media-processor board` *UUCSS*, where *UUCSS* is the location of the active circuit pack.

```
status media-processor board 1c03                                Page 1 of 1
                              MEDIA-PROCESSOR STATUS
Duplication State: active                   Duplication State: standby
   Board Location: 1c03                       Board Locations: 1c07
Source IP Address: 192.168.22.11           Source IP Address: 192.168.22.51
        Node Name: medpro1                          Node Name: medpro2
      Subnet Mask: 255.255.255.0                 Subnet Mask: 255.255.255.0
  Gateway Address: 192.168.22.255            Gateway Address: 192.168.22.255
      MAC Address: 00:00:04:0d:05:03              MAC Address: 00:00:04:0d:
05:07
 Ethernet Enabled? yes                       Ethernet Enabled? yes
                            COMMON DUPLICATED VALUES
   Links   Alarms     Standby Refreshed: yes     Locked? no   Links   Alarms
  mpcl: up mj: 0         Network Region: 1                   mpcl: up mj: 0
   eth: up mn: 0       Shared IP Address: 135.9.72.52          eth: up mn: 0
  peer: up wn: 0         Shared Virt-MAC: 02:00:04:0d:05:18   peer: up wn: 0
                               DSP CHANNEL STATUS
DSP 1: in-service/active, 60 calls          DSP 1: in-service/standby
DSP 2: in-service/active, 50 calls          DSP 2: in-service/standby
DSP 3: in-service/active, 57 calls          DSP 3: in-service/standby
DSP 4: in-service/active, 47 calls          DSP 4: in-service/standby
```

3. Look at the LINKS and DSP CHANNEL STATUS categories to determine whether the call is being processed.
4. Enter `set media-processor` *UUCSS*, where *UUCSS* is the location of the standby TN2602AP circuit pack.

   The standby TN2602AP circuit pack becomes active.
5. Enter `status media processor board` *UUCSS*, where *UUCSS* is the location of the newly-active circuit pack.

   The system displays the Media Processor Status window. Under DSP CHANNEL STATUS, the test call has moved to the column for the newly-active TN2602AP circuit pack.

**Note:**

TN2602AP call processing and interchange activity is tracked through the MEDPRO-C maintenance object. See *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*, 03-300430.

# Appendix A: Accessing the server

You must have access to the server for administration. The following computers and software are the supported access points for accessing the server for initial configuration, aftermarket additions, and continuing maintenance:

- Personal computers
- Services laptop computers equipped with a network interface card (NIC)
- Terminal emulation program
- Web browser

You can access the server either directly or remotely over the customer network or over a modem. Connecting directly and remotely over the customer network are the preferred methods. Remote access over a modem is for Avaya maintenance access only.

## Service laptop and server connection

You can connect a service laptop into the services port of a server to access the server directly. You can connect a service laptop directly to different servers, like S8300D, S8510, S8800, HP DL360 G7, and Dell R610. The diagrams in the following section illustrate the process for connecting the server laptop to the supported servers.

## Connecting a services laptop to an S8300D Server

### About this task

The following figure shows connection between a service laptop and the S8300D Server.

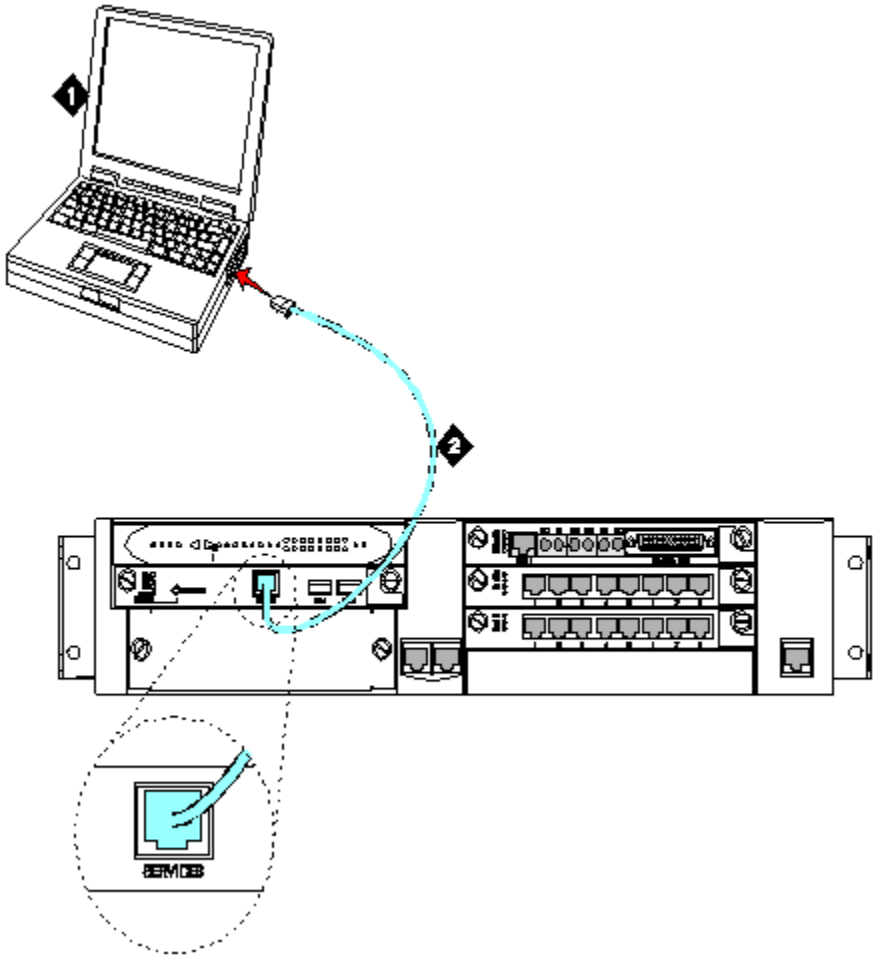


**Figure 9: A services laptop connected directly to an S8300D Server**

| Number | Description |
|---|---|
| 1 | Services laptop |
| 2 | Black CAT5 cross-connect cable |

# Connecting a services laptop to an S8510 Server

## About this task

The following figure shows connection between a service laptop and the S8510 Server.

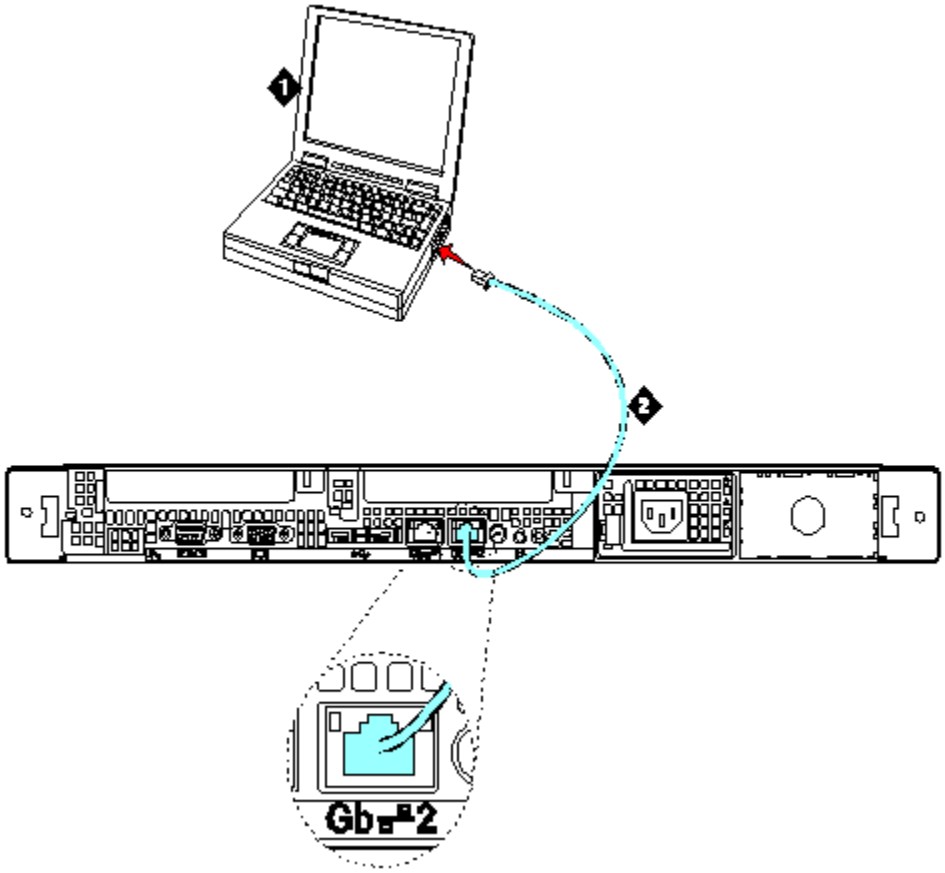


**Figure 10: A services laptop connected directly to an S8510 Server**

| Number | Description |
|---|---|
| 1 | Services laptop |
| 2 | Black CAT5 cross-connect cable |

# Connecting a services laptop to an S8800 Server

## About this task

The following figure shows connection between a service laptop and the S8800 Server.

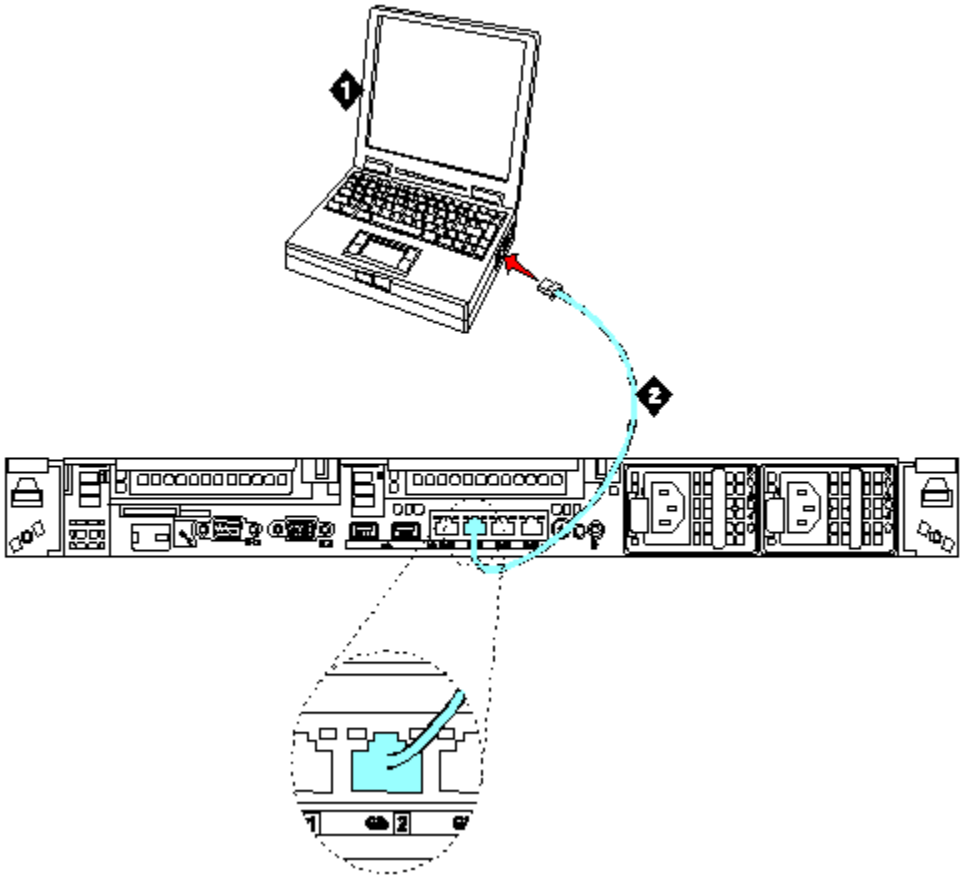

**Figure 11: A services laptop connected directly to an S8800 Server**

| Number | Description |
|---|---|
| 1 | Services laptop |
| 2 | Black CAT5 cross-connect cable |

# Connecting a services laptop to an HP DL360 G7 Server

## About this task

The following figure shows connection between a service laptop and the HP DL360 G7 Server.

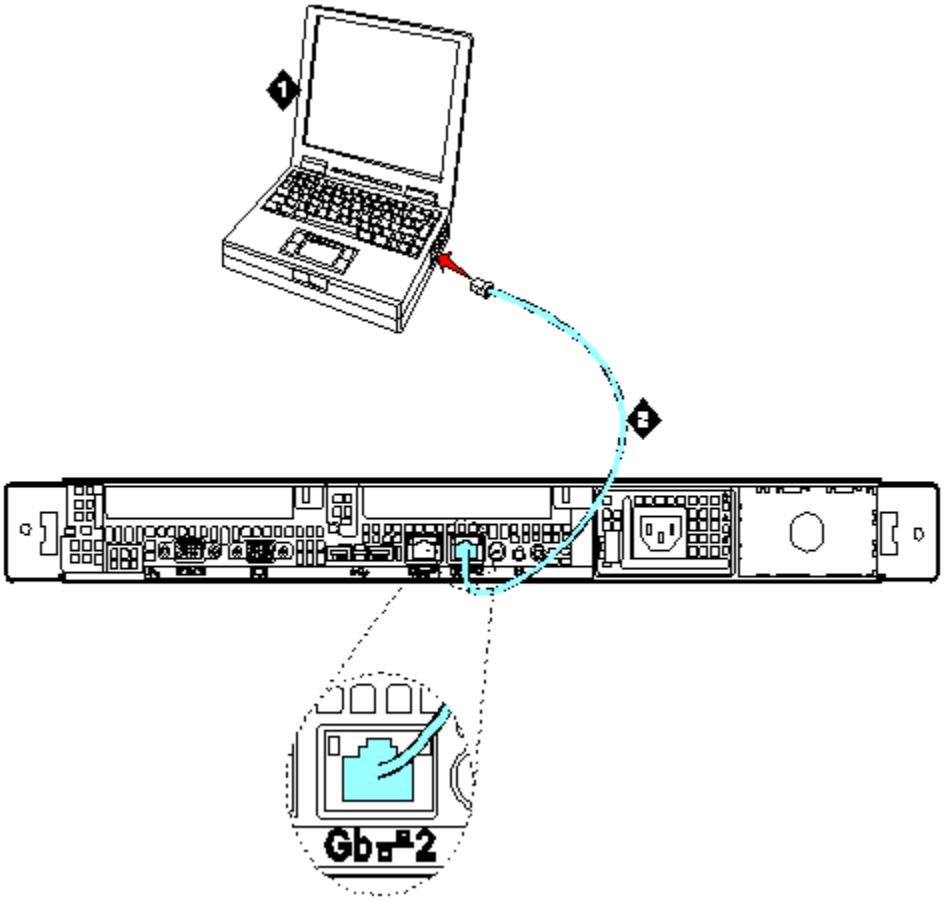


**Figure 12: A services laptop connected directly to an HP DL360 G7 Server**

| Number | Description |
|---|---|
| 1 | Services laptop |
| 2 | Black CAT5 cross-connect cable |

# Connecting a services laptop to an Dell R610 Server

## About this task

The following figure shows connection between a service laptop and the Dell R610 Server.

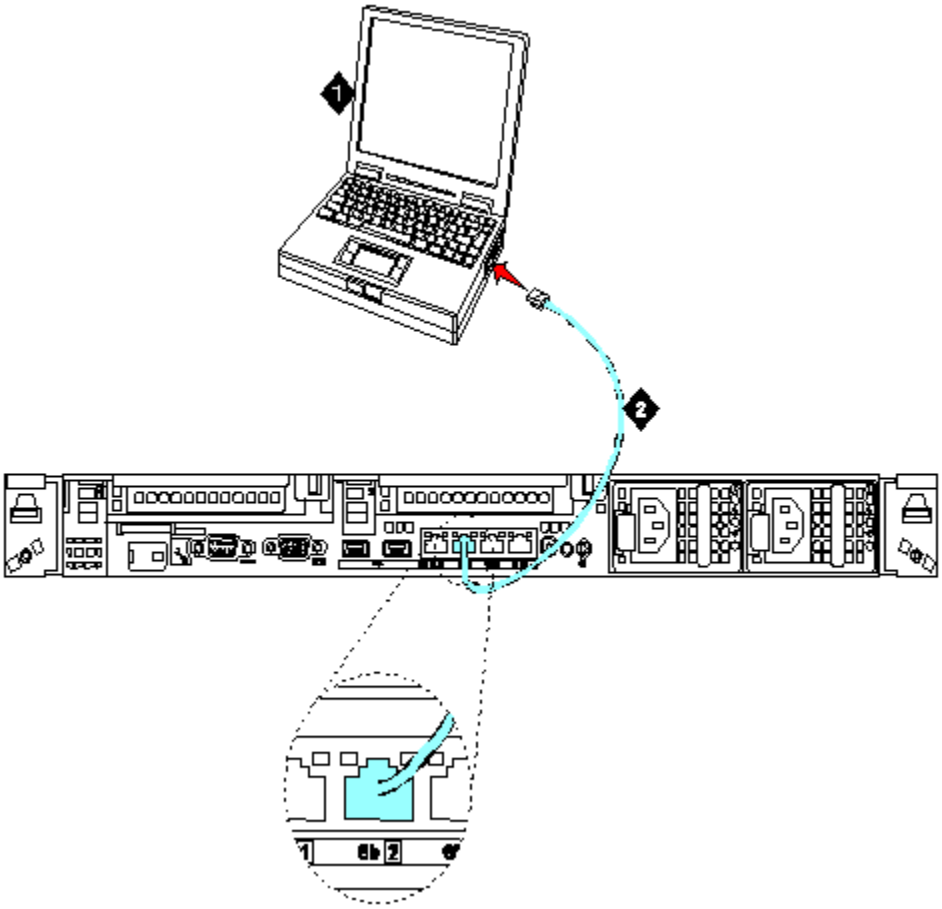


**Figure 13: A services laptop connected directly to an Dell R610 Server**

| Number | Description |
|---|---|
| 1 | Services laptop |
| 2 | Black CAT5 cross-connect cable |

# Server administration

## Finding the IP address of the active server (duplicated servers)

### About this task

To find the IP address of the active server in a configuration with duplicated servers, perform the following steps:

### Procedure

1. Go to the task bar at the bottom right of your personal computer.


2. Right-click the **Network Status** icon. Click **Status**, and then click the **Details** tab.
3. Scroll down until you see the Server IP address. This IP address is for the server to which you are connected.

## Disabling the boot timeout of the SAMP board

### About this task

To disable the boot timeout of the SAMP:

### Procedure

1. At the command line on the S8300D/S8800/S8510/HP DL360 G7/Dell R610 Server, enter `sampcmd`.

   The Welcome banner appears, followed by the SAMP command line.
2. At the SAMP command line, enter `serverctrl boot timer disable`.

   The system responds with `OK`.
3. At the SAMP command line, enter `serverctrl`.

   The system responds with the following output:

```
Power On
Server Operational
Reset Deasserted
Boot Time Disabled
```

4. Enter `Exit` to return to the server command line.

### Result

When you have completed the upgrade and the server reboots, the SAMP boot timeout is automatically enabled again.

**Note:**

You can also disable the boot timeout of the SAMP board by connecting to the SAMP services port and using the Web pages of the SAMP. For more information, see *Disabling*

*the boot timeout on Release 3.1 using the SAMP Web page* in the *Using the Avaya Server Availability Management Processor (SAMP), 03-300322*.

# Accessing System Management Interface directly

## About this task

To access System Management Interface directly, you can either connect:

- Directly to the services port on the server. For more information, see Service laptop and server connection on page 97.
- Over the customer network.

MS Internet Explorer 7.0 or later and FireFox 3.6 or later are the only browsers that are supported.

When you connect directly to the server, you must disable all proxy servers. For more information and instructions, see Connecting the browser directly to the server on page 18 and Connecting the browser remotely through the network on page 19.

To access System Management Interface (SMI):

## Procedure

1. Open the MS Internet Explorer or FireFox Web browser.
2. Perform one of the following actions:
   - If you want to connect directly, in the **Address** field, type `192.11.13.6`.
   - If you want to connect remotely, in the **Address** field, type the IP address or the DNS host name of the server.
3. When prompted, log in.

**Note:**

For Prerelease 5.2 use the Maintenance Web Interface, and for Release 5.2 use the System Management Interface (SMI).

# Accessing the server command line interface with ssh protocol

## About this task

- To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. In addition, a third-party ssh client must already be installed on your computer.
- PuTTY is one such client available for download from http://www.putty.nl/download.html. The following procedure describes, as an example of ssh access, how to log into the server command line with PuTTY.

**Note:**

A version of PuTTY that is defaulted for ssh server access is available for Avaya services personnel only. In this version, some values below have already been preselected.

**Caution:**

While a variety of Avaya products support access using ssh, Avaya does not provide support for third-party clients used for ssh access. Any problems with an ssh client, including PuTTY, are the responsibility of the user or the ssh client vendor.

To access the command line interface using PuTTY with ssh:

## Procedure

1. On your computer, click on the **PuTTY** desktop link or select **Start** > **Programs** > **PuTTY** > **PuTTY**.
2. In the **Host Name** (or **IP address**) field, type `192.11.13.6` if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.
3. In the **Port** field, type `22` (the SAT is 5022).
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection** > **SSH**.
   The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select 2.
7. In the Encryption options window, use the up and down arrows to set AES (SSH-2) as the top option and 3DES as the second option.

   **Note:**

   You can save the PuTTY settings and customize the PuTTY tool with other settings, such as for color. For documentation on PuTTY, see http://www.putty.nl/docs.html.

8. In the PuTTY menu on the left, click **Terminal** > **Keyboard**.
   The Options controlling the effects of keys dialog box opens.
9. In the Backspace key area, select **Control-H**.
   This activates the backspace key while you are using the SAT.
10. Click **Open**.

    **Note:**

    If you have not connected to this particular server before, ssh prompts you to accept the server host key. If you save this key when prompted, you will not be prompted if you connect again later. If you do not save the key, PuTTY prompts you the next time you connect to this server.

    When connecting through the Services laptop interface on the server, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as 192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.
11. If necessary, click **Yes** to accept the server's host key.
12. Log in to the server.

# Accessing the command line interface with terminal emulation

## About this task

To use a command line interface in a terminal emulation window:

**Note:**

Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are the only supported terminal emulation programs.

## Procedure

1. Open your terminal emulation application.
2. Ensure that the port settings of the terminal emulation program are configured as follows:
   - 115200 baud
   - No parity
   - 8 data bits
   - 1 stop bit

- No flow control

3. Establish a network connection to the server with either the IP address or the DNS host name. Use port 5023 for this connection.
4. When prompted, log in.

# Logins

Initial configuration and upgrades by an Avaya technical support representative or an Avaya Business Partner requires a services login, such as craft or dadmin. Avaya technical support representatives can also use a unique password that is assigned to that customer system.

When you finish installing the Avaya authentication file, Communication Manager has a password for the craft login. This password is unique to the server of the customer. You can use the password the next time that you log in as craft, if you access the server through the Services port. Every other means of craft access still requires an ASG challenge/response. RFA records the revised password. ASG Interactive Response provides this password at 1-800-248-1234 or 1-720-444-5557.

You have to obtain logins and passwords for the following components:

- Server
- Gateway
- IPSI
- auxiliary equipment
- Communication Manager

Customers can set up their own logins to access Avaya servers. For more information, see the *Administering Avaya Aura® Communication Manager*, 03-300509. You must have superuser permission to create or change logins and passwords.

**Important:**

When you assign login IDs, do not start the logins with a number.

# Index

## D



## E



## F



## G



## H



## I

## L



## M



## N



## P



## R



## S

## T



## U



## V



## W