



**Installing and Configuring the
Avaya S8700-Series Server**
Release 5.2

03-300145
Release 5.2
May 2009
Issue 8

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.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Websites referenced within this site or documentation(s) 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.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Website: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

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, and 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 End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS):
End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, 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.

- Named User License (NU):
End User 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 (for example, 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):
Customer 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"). (See Third-party Components for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Website: <http://support.avaya.com/Copyright>.

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 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://www.support.avaya.com/>.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) 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(s) 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. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Website: <http://www.avaya.com/support>.

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

Disclaimer

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: <http://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 or IEC 60950-1, including all relevant national deviations as listed in the IECCE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950 / UL 60950 or CAN/CSA-C22.2 No. 60950-1 / UL 60950-1.

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:

A. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:

- answered by the called station,
- answered by the attendant,
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
- Routed to a dial prompt

B. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products

approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

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

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

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

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

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

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

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

Installation and Repairs

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

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

FCC Part 68 Supplier's Declarations of Conformity

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

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

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

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

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

European Union Declarations of Conformity



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

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

European Union Battery Directive



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

Japan

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用する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。

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

<http://www.avaya.com/support>

Contents

Chapter 1: Introduction	11
Audience	11
How to use Avaya installation documents	12
PNC license settings for S8700-series Servers	13
Preinstallation tasks to complete at the customer site	13
Verifying that all the required equipment is on site	13
Ensuring that the preinstallation tasks are complete	13
Equipment specifications	14
About S8730 Server configurations	17
About RAID	17
About server port connections	17
S8700-series port connections	18
About modem connections	23
Modem options	24
About media gateways	24
About Processor Ethernet	24
About software duplication	25
About SSH	25
Chapter 2: SNMP configuration	27
Configuring the SNMP modules in the UPS	27
Default UPS IP addresses for S8700-series Servers	28
Prerequisites for configuring the SNMP module	29
Administering the SNMP modules	30
Setting selected traps (alarming)	30
Configuring the SNMP subagent in the Avaya Ethernet switch (if used)	31
Default IP addresses for the Ethernet switch	31
Preparing to configure the Ethernet switch	32
Configuring the Ethernet switch	33
Chapter 3: Communication Manager installation	35
Clearing the ARP cache on the laptop	35
Applying power to the server	36
Accessing the server	36
Configuring Telnet for Windows 2000 and Windows XP	36
Installing Communication Manager	37

Chapter 4: Server configuration	39
Methods of Configuring a server	39
Opening the System Management Interface	40
Creating a super-user login	40
Installing the license and authentication files	41
Installing the license file	41
Installing the authentication file	41
Configuring the server manually	42
Setting the date, time, and time zone	42
Rebooting the server	42
System Management Interface configuration screens	43
Ethernet interface assignments	44
Performing the manual configuration	45
Avaya Installation Wizard	46
About the Avaya Installation Wizard	46
Running the Avaya Installation Wizard	47
Verifying the server connection to the customer LAN (if provided)	47
Configuring the modem	48
Configuring memory for an S8720 Server	49
Ensuring ESS and LSP compatibility	50
Enabling firewall settings	51
Enabling network time servers	51
Configuring the NIC	52
Release the server	53
Configuring a second server	53
Interchanging servers	53
Accessing the standby server	53
Interchanging servers	54
Performing an integrity check on the active server	54
Chapter 5: IP interface translations	57
Inputting initial system translations	57
Adding media gateways	58
Enabling the IPSI	59
Adding the IPSI to the system	60
Enabling IPSI duplication (duplicated control network only)	61
Setting the alarm activation level	61
Saving translations	61

Verifying connectivity to the server	62
Verifying that the IPSIs are translated	62
Upgrading the IPSI firmware version (if necessary)	62
Enabling control of the IPSIs	63
Verifying the license status	63
Chapter 6: IP interface configuration	65
Connecting to the IPSIs	65
IPSI address configuration	65
Programming the IPSI for static addressing	66
Setting the VLAN and diffserv parameters	68
Programming the IPSI for DHCP addressing	70
Chapter 7: Postinstallation administration	73
Verifying translations	73
Setting rules for daylight savings time	74
Setting locations (if necessary)	75
Verifying the date and the time (main server only)	76
Clearing and resolving alarms	77
Enabling and disabling the Ethernet switch ports	77
Enabling alarms to INADS by way of a modem	79
Enabling alarms to INADS by way of the SNMP module	80
Backing up files to the compact flash media	80
Before leaving the site	81
Chapter 8: Installation verification	83
Testing the IPSI circuit pack	83
Testing the license file	83
S8730 LEDs	84
S8710 and S8720 LEDs	86
Additional server LED information	88
Avaya C360 Ethernet switch LEDs	89
UPS LEDs	90
TN2312BP IPSI LEDs	91
Appendix A: Server access	95
Accessing the command line interface of the server with SSH	95

Contents

Connecting to the server directly	97
Connecting to the server remotely over the network	100
Connecting to the server remotely over a modem	100
Finding the IP address of the active server	101
Accessing the System Management Interface	101
Accessing the SAT.	103
Logins for Avaya technicians and Business Partners	103
Configuring the network for Windows 2000 and XP	104
Setting the browser options for Internet Explorer 6.0	105
Appendix B:	
Installation troubleshooting	107
Troubleshooting the installation of the server hardware	107
Troubleshooting the configuration of the server hardware	108
Troubleshooting the installation of the license file and the Avaya authentication file	110
.	111
.	113
.	115
.	117
Index	119

Chapter 1: Introduction

Use these procedures to install Avaya Communication Manager and configure a new Avaya S8700-series Server and the associated components in a fiber-connected (fiber-PNC) or an IP-connected (IP-PNC) port network configuration.

To configure the server, use the Avaya Installation Wizard. To configure gateways and other hardware components, use the following two administration interfaces:

- 1 The System Management Interface.
- 1 The command line interface, either directly or through Secure Shell (SSH), Telnet, or a terminal emulation program such as Avaya Native Configuration Manager.

This installation document includes the following information:

- 1 [Preinstallation tasks to complete at the customer site](#) on page 13
- 1 [Configuring the SNMP modules in the UPS](#) on page 27
- 1 [Server configuration](#) on page 39
- 1 [IP interface translations](#) on page 57
- 1 [IP interface configuration](#) on page 65
- 1 [Postinstallation administration](#) on page 73
- 1 [Installation verification](#) on page 83
- 1 [Server access](#) on page 95
- 1 [Installation troubleshooting](#) on page 107

Audience

This documentation is for the following people who install and configure the server components:

- 1 Trained field installation and maintenance personnel
- 1 Technical support personnel
- 1 Authorized business partners

How to use Avaya installation documents

Use this document as a guide to install and configure the S8500 Avaya servers. For information about a particular task, use the index or the table of contents to locate the page on which the information is described. You also need information from other Avaya documents. This section lists those documents and tells you when to use them.

To complete this installation:

- 1 In this document, see:
 - [Preinstallation tasks to complete at the customer site](#) on page 13. This section describes the tasks that you must complete before you start the installation.
 - [Equipment specifications](#) on page 14 for the technical specifications for the hardware.
- 1 For how to install and connect the hardware, see *Quick Start for Hardware Installation: Avaya S8700-Series Server* (555-245-701).
- 1 Return to this document and see the remaining sections in the following sequence to install the components of the server. If you are not to install certain components, skip the procedures for those components.
 - [Configuring the SNMP modules in the UPS](#) on page 27
 - [Server configuration](#) on page 39
 - [IP interface translations](#) on page 57
- 1 See the appropriate sections in the following documents to install the port networks and the media gateways:
 - *Installing the Avaya G650 Media Gateway* (03-300144)
 - *Installation and Configuration for the Avaya G150 Media Gateway* (03-300395)
 - *Quick Start for Hardware Installation: Avaya G250 Media Gateway* (03-300433)
 - *Quick Start for Hardware Installation: Avaya G350 Media Gateway* (03-300148)
 - *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)
 - *Installing and Upgrading the Avaya G430 Media Gateway* (03-603233)
 - *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
 - *Installing and Upgrading the Avaya G250 Media Gateway* (03-300434)
 - *Installing and Upgrading the Avaya G350 Media Gateway* (03-300394)
 - *Installing and Upgrading the Avaya G450 Media Gateway* (03-602054)
 - *Quick Start for Hardware Installation: Avaya S8300 Server and Avaya G700 Media Gateway* (555-233-150)
 - *Installation and Upgrade for the Avaya G700 Media Gateway and Avaya S8300 Server* (555-234-100)
 - *Installation and Initial configuration of Avaya Aura™ Communication Manager Messaging*

- Return to this document and see: [IP interface configuration](#) on page 65 to program the IP interface. [Postinstallation administration](#) on page 73
- [Installation verification](#) on page 83
- [Server access](#) on page 95
- [Installation troubleshooting](#) on page 107 if problems occur during the installation.

PNC license settings for S8700-series Servers

For Communication Manager Release 4.0 and later releases, the two major types of port network connectivity, IP-PNC and fiber-PNC (also called multiconnect), are both automatically enabled in all licenses for S8700-series Server. As a result, unlike the license settings in previous releases, platform 8 for IP-PNC and the Internet Protocol (IP) PNC feature attribute are no longer needed and are not available as license options. For Release 4.0 and later releases, you always select platform 6, multiconnect, in a license for an S8700-series Server.

Preinstallation tasks to complete at the customer site

You must complete the following preinstallation tasks before you start the installation.

- 1 Install the DAL2 card, if used

Verifying that all the required equipment is on site

Compare the list of items that were ordered to the contents of the boxes to verify that you have all the equipment. Your project manager can give you an inventory list. Do not rely on the packing slips inside the boxes for the correct information.

Ensuring that the preinstallation tasks are complete

The preinstallation team completes the following tasks. If these tasks are not complete, do not continue with the installation.

- 1 Verify that the required number of open, customer-supplied, EIA-310D (or equivalent) standard 19-in. (48-cm) 4-post equipment rack(s) is(are) properly installed and solidly secured. Ensure that the screws that come with the racks are present. If you use an enclosed rack cabinet, ensure that the cabinet has adequate ventilation.

- 1 Verify that the rail kit to support the server is available to install (S8400 installed in a G650 carrier only).
- 1 Verify that the rail kit to support the server is available to install.
- 1 Verify that the rail kit that is required to support the UPS is installed on the rack or available to install. For how to install the rails, see the documentation that comes with the rail kit.
- 1 Verify that the equipment racks are grounded per local code. See *Job Aid: Approved Grounds* (555-245-772).
- 1 Verify that the customer-provided AC power to the rack is from a nonswitched outlet.
- 1 Verify that cables for the TN2312BP (IPSI) circuit packs are labeled and run from the control hardware rack to the port networks or that appropriate connectivity is provided.

Equipment specifications



Important:

The TN8400BP circuit pack is compatible with Communication Manager Release 4.0.3 and later.

The components of the S8700-series Server control network consist of two servers, one or two Ethernet switches, and two UPSs. The physical specifications for the control network components are shown in [Table 1](#).

Table 1: Control network components specifications

Component	Dimensions English (height x width x depth in inches)	Dimensions Metric (height x width x depth in centimeters)	Height (u)	Weight (lb/kg)
Server S8710, S8720, or S8730	3.4 x 17.5 x 26	8.6 x 45 x 66	2	60/27 (loaded)
Ethernet switch: C363T	1.75 x 17 x 14.4	4 x 43 x 37	1	11/5
C364T	1.75 x 17 x 14.4	4 x 43 x 37	1	11/5
UPS: 1000 VA	3.4 x 17.2 x 17.7	9 x 43 x 45	2	49.4/22.4
1500 VA	3.5 x 17 x 24	9 x 43 x 61	2	50/23

[Table 2](#) shows specifications for the S8710, S8720 and S8730 Servers.

Table 2: S8710, S8720 and S8730 Server features and specifications

Feature	Description
Microprocessor	S8710: 1 Intel Xeon S8720: 1 AMD Opteron S8730: 1 Dual Core rev "F" AMD
Memory	S8710: 512 MB S8720: 1 GB S8730: 4 GB
Drives (SCSI)	Hard disk drive: 72 GB, 10,000 RPM CD-ROM/DVD-ROM: 24x maximum Diskette drive: 1.44 MB (3.5 in. [9 cm])
DAL2 hardware duplication cards	Used for the hardware duplication configuration only. Not used for the software duplication configuration.
Physical dimensions	S8710/S8720: Height: 3.4 inches [8.6 cm], 2 U) Depth: 26 inches (66 cm) Width: 17.5 inches (45 cm) Maximum weight: 60 lb (27 kg) S8730: Height: 3.38 inches [8.59 cm], 2 U) Depth: 26.01 inches (66.07 cm) Width: 17.54 inches (44.54 cm) Maximum weight: 60 lb (27.22 kg)
Integrated functions	S8710/S8720: 2 10/100/1000BaseT Ethernet connectors S8730: 2 100/1000Gb Ethernet ports Serial connector iLO connector (unused) Keyboard connector Mouse connector USB connectors: S8710: 2 S8720: 3 S8730: 4 Video connector VHDCI SCSI connector

Environmental specifications for the S8710, S8720 and S8730 are shown in [Table 3](#).

Table 3: S8710/S8720/S8730 Server environmental specifications

Parameter	Description
Air Temperature	<p>Ambient operating: 50°F to 95°F (10°C to 35°C) Maximum wet bulb: 82.4°F (28°C) NOTE: All temperature ratings shown are for sea level. An altitude derating of 1.8°F per 1000 ft to 10,000 ft (1°C per 300 meters) is applicable. No direct sunlight is allowed.</p>
Humidity	<p>Operating: 10% to 90% Nonoperating: 5% to 85% (S8730: 5% to 95%) NOTE: The storage maximum humidity of 95% is based on a maximum temperature of 113°F (45°C). The altitude maximum for storage corresponds to a pressure minimum of 70 kPa.</p>
Electrical input	<p>Rated input voltage: S8710/8720: 100 VAC to 240 VAC S8730: 100 to 132 VAC, 200 to 240 VAC Rated input frequency: 50 Hz to 60 Hz Rated input current: S8710/8720: 6 A (110 V) to 3 A (220 V) S8730: 10 A at 100 VAC, 4.9 A at 200 VAC Rated input power: S8710/8720: 600 W S8730: 980 W at 100V AC input 960 W at 200V AC input BTUs per hour: 2050</p>
Power supply output	<p>Rated steady-state power: S8710/8720: 400 W S8730: 800 W at 100V AC input 850 W at 120V AC input 1000 W at 200V to 240V AC input Maximum peak power: S8710/8720: 400 W</p>

About S8730 Server configurations

The S8730 Server comes with the option of two hard disk drives. In configurations with two hard drives, the RAID level 1 feature is enabled, so that disk mirroring automatically creates a complete set of data on both disks.

For different configurations of the S8730 Server:

- 1 If the server has only one hard drive, the drive should be in bay 1 (the leftmost bay)
- 1 If the server has two hard drives, the drives should be in bay 1 and bay 2.

After installation, do not attempt to move a drive from one bay to the other. If movement of drives is necessary, the server must be reinstalled.

About RAID

One or more hard drives may be added to an S8730 Server in order to take advantage of the RAID level 1 feature, which provides disk mirroring. In this configuration, a customer's data is mirrored on two disks, thus increasing the availability of the system. Each of the disks is independent of each other and contains a complete copy of the data. No administration is necessary to activate the RAID feature. Once an additional hard drive is installed, Communication Manager recognizes the additional hard drive and automatically activates RAID.

Note:

The RAID level 1 feature is only available on S8730 Servers.

About server port connections

The following section explains how to connect the Ethernet ports on the back of the server.

S8700-series port connections

The network cable connections depend on the type of server, type of memory duplication, and the type of control network. All cables are CAT5 or better patch cables except for the fiber cable that interconnects the DAL2 cards for hardware duplication.

- 1 For a guide to connect the cables to the servers for hardware duplication on the S8730 Server, see [Figure 1: Duplication and control network cabling for hardware duplication \(S8730\)](#) on page 19.
- 1 For a guide to connect the cables to the servers for hardware duplication on the S8720 or S8710 Server, see, [Figure 2: Duplication and control network cabling for hardware duplication \(S8720/S8710\)](#) on page 20.
- 1 For a guide to connect the cables to the servers for software duplication on the S8730 Server, see [Figure 3: Duplication and control network cabling for software duplication \(S8730\)](#) on page 21.
- 1 For a guide to connect the cables to the servers for software duplication on the S8720 or S8710 Server, see, [Figure 4: Duplication and control network cabling for software duplication \(S8720/S8710\)](#) on page 22.

Figure 1: Duplication and control network cabling for hardware duplication (S8730)

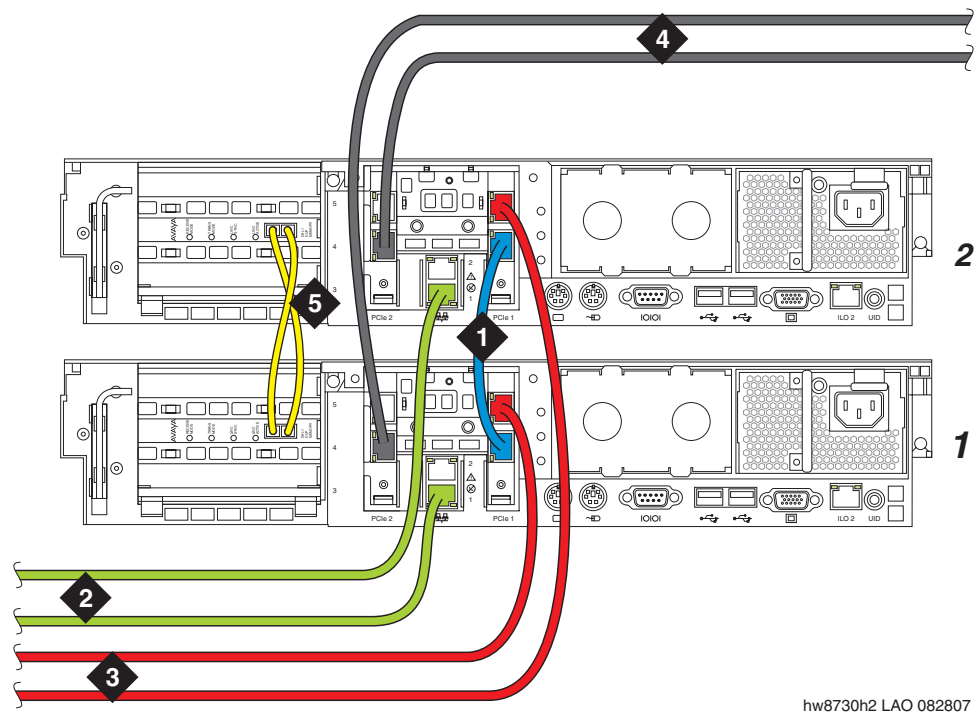


Figure notes:

1. Eth2 — Server duplication link - duplication crossover cable
2. Eth0 — CNA (also LAN for nondedicated control network)
3. Eth3 — To an Ethernet switch and/or the corporate LAN for control network B (CNB)
4. Eth4 — To the customer LAN if the control networks are dedicated
5. Fiber duplication cable

Note:

These are typical Ethernet port assignments. The customer might specify different assignments for Eth0, Eth2, Eth3, and Eth4.

Figure 2: Duplication and control network cabling for hardware duplication (S8720/S8710)

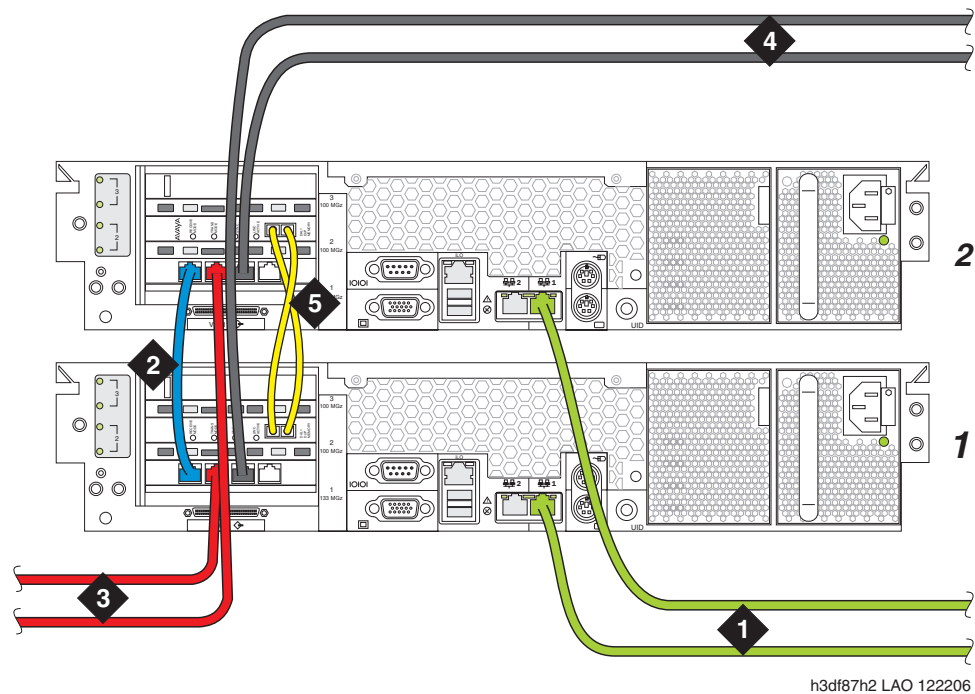
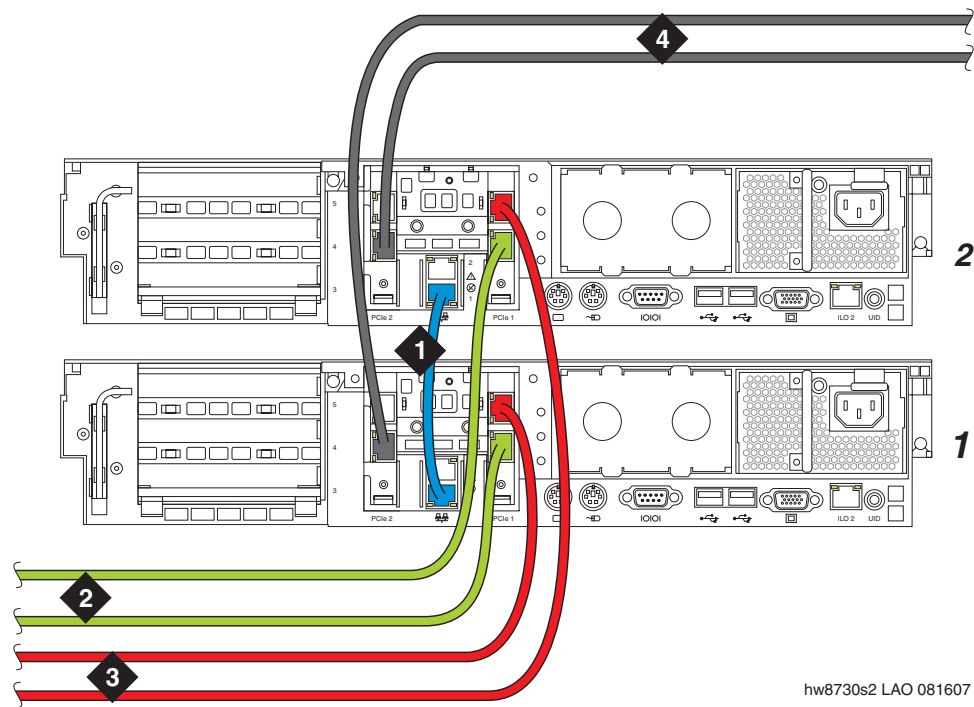


Figure notes:

1. Eth0 — To an Ethernet switch and/or the corporate LAN for control network A (CNA)
2. Eth2 — Server Duplication Link
3. Eth3 — To an Ethernet switch and/or the corporate LAN for control network B (CNB)
4. Eth4 — To the customer LAN if the control networks are dedicated
5. Fiber duplication cable

Note:

These are typical Ethernet port assignments. The customer might specify different assignments for Eth0, Eth2, Eth3, and Eth4.

Figure 3: Duplication and control network cabling for software duplication (S8730)**Figure notes:**

1. Eth0 — Server Duplication Link - duplication crossover cable
2. Eth2 — To an Ethernet switch and/or the corporate LAN for control network A (CNA)
3. Eth3 — To an Ethernet switch and/or the corporate LAN for control network B (CNB)
4. Eth4 — To the corporate LAN if the control networks are dedicated.

Note:

These are typical Ethernet port assignments. The customer might specify different assignments for Eth2, Eth3, and Eth4.

Figure 4: Duplication and control network cabling for software duplication (S8720/S8710)

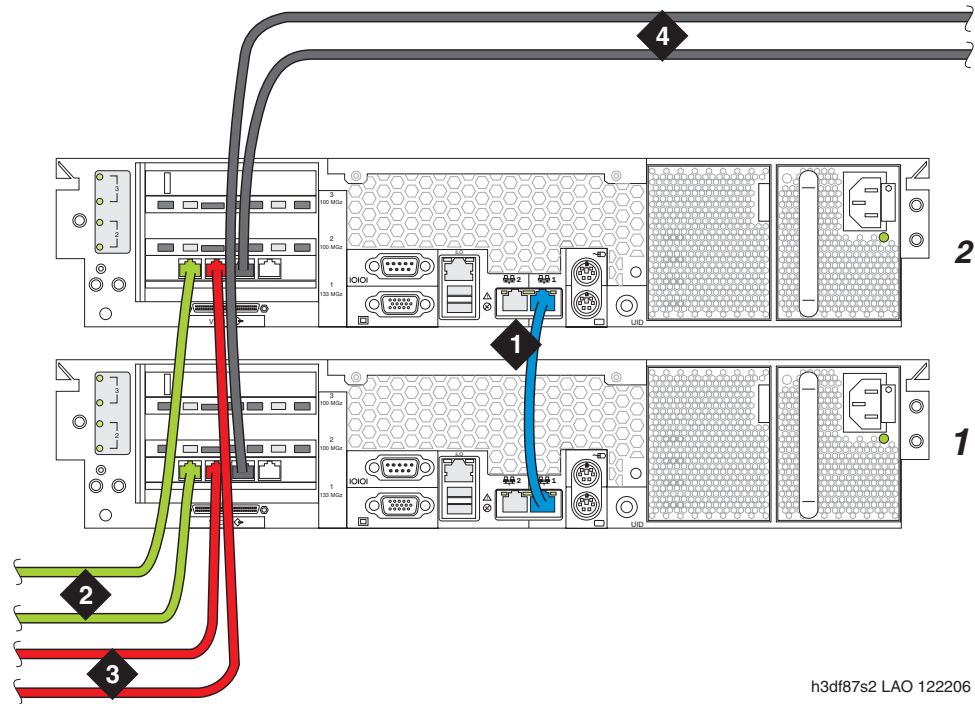


Figure notes:

1. Eth0 — Server Duplication Link
2. Eth2 — To an Ethernet switch and/or the corporate LAN for control network A (CNA)
3. Eth3 — To an Ethernet switch and/or the corporate LAN for control network B (CNB)
4. Eth4 — To the corporate LAN if the control networks are dedicated.

Note:

These are typical Ethernet port assignments. The customer might specify different assignments for Eth2, Eth3, and Eth4.

About modem connections

Note:

You cannot connect USB modems to rotary lines. A touch tone line is required.

On S8700-series Servers, connect a USB modem to the USB port on each server.



CAUTION:

Once you connect the modems to the servers, do not unplug the modem USB cable on the *active* server. If you must replace the modem, replace the modem when the server is in standby mode.

Connecting to collocated servers



Important:

Both servers share one telephone line.

To connect modems to collocated servers:

1. Install two RJ11 jack outlets wired to a single (1-Measured Business) telephone line.
2. Use the modular telephone cord that is supplied with the modem to connect one RJ11 jack to each modem.
3. Use the USB cable that is supplied with the modem to connect one modem to server 1.
4. Use the USB cable to connect the other modem to server 2.

Connecting to separated servers



Important:

Each server has a dedicated telephone line.

To connect to separated servers:

1. For a server in each location, install one RJ11 jack outlet that is wired to a single 1-Measured Business telephone line.
2. Use the modular telephone cord that is supplied with the modem to connect one RJ11 jack to each server.
3. Connect each modem, using the USB cable, to the server at each location.

Modem options

You set the modem options when you configure the server. You must not set options on the modems themselves. For information about modem option settings, see *Installation, Upgrades and Additions for Avaya CMC1 Media Gateways* (555-233-118).

About media gateways

In a new installation, the S8700-series Servers work with only the Avaya G650 Media Gateway.

In a migration, the S8700-series Servers work with Avaya MCC1 and SCC1 Media Gateways in a fiber-PNC configuration and G600 or CMC1 Media Gateways in an IP-PNC configuration.

The servers also work with Avaya G150, G250, G350, G430, G450, and G700 Media Gateways. These gateways register with the server either through the Processor Ethernet interface or through a TN799DP C-LAN circuit pack.

Media gateways usually are installed in the same equipment room as the server rack hardware or control network. However, you can install the media gateways in another location, including another state or country.

About Processor Ethernet

Like a C-LAN circuit pack, Processor Ethernet provides connectivity to IP endpoints, gateways, and adjuncts. The PE interface is a logical connection in the Communication Manager software that uses a port on the NIC in the server. No additional hardware is needed to implement PE.

Starting with Release 3.1 of Communication Manager, the PE interface is enabled on the S8700-Series Server to allow enhanced flexibility to connect to gateways, endpoints, and adjuncts.

The PE interface is always enabled on an S8700-series Server pair for registration by an ESS or an LSP. However, the PE interface is not supported on duplex servers for registration by an H.248 gateway, H.323 endpoints, or adjuncts.

About software duplication

Software duplication eliminates the need for the DAL2 duplication cards in duplicated S8720 and S8730 Servers. Software duplication is supported only on the S8720 and S8730 and is the default configuration. For software duplication, all duplication messages are sent over the server duplication TCP/IP link.

An S8720 or S8730 communications system configured with software duplication has lower call performance than the same system configured with hardware duplication. Encrypting duplication messages further degrades performance. For software duplication, Avaya recommends that you use a dedicated duplication link with a bandwidth of at least 1 Gigabit per second.

The S8720 and S8730 Server is shipped without the optional DAL2 hardware duplication card. If purchased, the DAL2 hardware duplication cards and the dual fiber cable that links the DAL2 cards are installed in the servers at the customer site.

The duplication type, that is, hardware or software, is administered as a Configure Server step on the Server Duplication Web page in the System Management Interface.

About SSH

Secure Shell (SSH) is both a computer program and an associated network protocol that you use to log in to and run commands on a networked computer. SSH provides secure encrypted communications between two untrusted hosts over an insecure network. Avaya strongly recommends that you use SSH instead of Telnet for most interactive connections to the Avaya servers and other devices on a customer network.

To use SSH, a third-party SSH client must be installed on your computer. PuTTY is one such client. You can download PuTTY from <http://www.putty.nl/download.html>.

You can use SSH to access the following devices:

- 1 The S8300, S8400, S8500, and S8700-series Servers on Release 3.1 or later of Communication Manager
- 1 A TN2312BP IPSI that is running firmware version 20 or higher
- 1 A TN2602 IP Media Resource that is running the latest firmware version. To find the latest firmware version, visit support.avaya.com
- 1 An Expanded Meet-Me Conferencing (EMMC) server
- 1 A SIP Enablement Services (SES) server
- 1 G250, G350, and G450 media gateways
- 1 C360 Ethernet switches

**Important:**

You cannot use SSH with the G700. From within the Linux command line of a server, you can use SSH to access the G250, 350, and G450, but you must use Telnet to access the G700.

Chapter 2: SNMP configuration

After you install and connect the control network equipment, you must configure the SNMP modules in each Avaya-supplied UPS to send alarms or traps to the servers. This process requires that you also configure the SNMP subagent in the Avaya-supplied Ethernet switch.

**Important:**

Use the procedures in this section to configure Avaya-supplied equipment only.

Configuring the SNMP modules in the UPS

**Important:**

These procedures apply only to a new, Avaya-supplied uninterruptible power supply (UPS) with a Simple Network Management Protocol (SNMP) module. Do not use these procedures to set traps on a UPS that Avaya does not supply. For non Avaya supplied UPS hardware, see manuals supplied with the UPS for instructions on how to configure those UPS devices.

You must configure the SNMP module in the UPS to report alarms to the server when hardware problems occur. The module reports an alarm if commercial power is lost or battery resources are depleted.

For the SNMP module to properly report alarms, you must configure a unique IP address for the UPS on both the SNMP module and the server. This IP address can be a customer-provided address or the Avaya-provided default address. At a minimum, you must configure the following items:

- 1 The IP address
- 1 The subnet mask
- 1 The gateway IP address
- 1 The trap receiver IP address
- 1 The community string (get, set, trap)

The brand, the model, or the firmware load of the SNMP module that Avaya supplies can change without notice because a third-party manufactures the SNMP module. For this reason, this document does not provide specific instructions on how to connect to and configure the SNMP module. For more information, see the documentation that comes with the SNMP module. For the default password and the configuration commands, see the local configuration section of that user guide.

Default UPS IP addresses for S8700-series Servers

For how to administer the SNMP module in the UPS, see. Perform the same steps for each UPS. [Table 4: Default UPS IP addresses for a dedicated control network](#) shows the default values for UPS1 and UPS2 for a dedicated control network. For non-dedicated control networks, the customer provides IP addresses.



Important:

Do not use the IP address of the active server.

Table 4: Default UPS IP addresses for a dedicated control network

Parameter	UPS	Single control network (CNA)	Duplicated control network (CNB)
IP address	UPS 1	198.152.254.239	198.152.255.239
Subnet mask		255.255.255.0	255.255.255.0
Gateway address	UPS 1	198.152.254.201	198.152.255.201
IP address for the trap receiver (server 1)	UPS 1	198.152.254.201	198.152.255.201
IP address	UPS 2	198.152.254.238	198.152.255.238
Subnet mask		255.255.255.0	255.255.255.0
Gateway address	UPS 2	198.152.254.201	198.152.255.201
IP address for the trap receiver (server 2)	UPS 2	198.152.254.202	198.152.255.202



Important:

Each UPS must report SNMP traps to the server that the UPS powers.

If the UPS detects that commercial power is lost or battery resources are depleted, the UPS sends a trap that allows the server to lower its state of health and to cause an interchange. If the UPS sends the trap to the wrong server trap receiver address, that server interchanges to the server that is plugged into the failing UPS. Thus, server 1 must be plugged into UPS1, and UPS1 *must* be configured to report SNMP traps to the actual IP address, and not the active server address, of server 1. The same requirements apply to server 2 and UPS2.

Prerequisites for configuring the SNMP module

Before you configure the SNMP module, you must complete the following prerequisites:

- 1 Your Services laptop computer is plugged into the correct administration port on the SNMP module on the UPS.
- 1 The UPS is plugged into a nonswitched electrical outlet.
- 1 The communication protocol on your computer has the following port settings so that you can use your terminal emulation program:
 - 9600 baud
 - No parity
 - 8 data bits
 - 1 stop bit
 - No flow control

Note:

Avaya Terminal Emulation and HyperTerminal are supported terminal emulation applications.

- 1 If a Network Management System (NMS) is used to monitor the UPS, you must coordinate the assignment of community names with the network administrator. If an NMS is not used, you can set the community names to any unique string values.



SECURITY ALERT:

The Get and Set community name strings are initially configured with the default values of Public and Private, respectively. These community name strings function as passwords for their respective SNMP operation. Avaya recommends that you change these community name strings to something other than the default values. If you leave the defaults in place, a serious security issue can result.

For information about which traps to set, see [Setting selected traps \(alarming\)](#) on page 30.

- 1 If the control network is nondedicated, ensure that the 162/udp port for input to server is enabled and the default is disabled. If you do not enable the 162/udp port and disable the default, the server cannot receive the traps from either UPS. See [Enabling firewall settings](#) on page 51.

Administering the SNMP modules

Note:

Use the default IP addresses.

1. Connect the RS-232 serial port of your Services laptop computer to the DB-9 connector on the back of the SNMP module for UPS1 using the DB-9 to DB-9 serial cable that is supplied with the SNMP module.
2. Open a VT-100 terminal emulation session on your computer.
3. Set the IP address for the UPS.
4. Set the subnet mask for the UPS.
5. Set the gateway address for the UPS.
6. Set the IP address of the trap receiver for the UPS.
7. Set the SNMP community name string for Get, Set, and Trap. For information on which traps to set, see [Setting selected traps \(alarming\)](#) on page 30.
8. When finished, disconnect your computer from the UPS.
9. Connect one end of a CAT5 straight-through cable to the RJ45 connector on the UPS1 SNMP module and the other end of the cable to the next available port on the Ethernet switch for Control Network A (CNA).

For a connectivity guide, see the *Quick Start for Hardware Installation: Avaya S8700 Series Server* (555-245-703).

10. Repeat Steps 1 through 8 for the SNMP module in UPS2.
11. For UPS2, connect one end of a CAT5 straight-through cable to the RJ45 connector on the UPS2 SNMP module. Connect the other end of the cable to the next available port on the Ethernet switch for Control Network B (CNB).

For a connectivity guide, see the *Quick Start for Hardware Installation: Avaya S8700 Series Server* (555-245-703).

After you configure the SNMP module in the UPS, you must configure the SNMP subagent on the Avaya Ethernet switch.

Setting selected traps (alarming)

The default is to set all traps, which can result in large log entries. To avoid this problem, Avaya recommends that you set only the following traps:

- 1 UPS on Battery—Indicates an AC power failure. Based on the level of battery reserve, a shutdown is pending.
- 1 UPS in Bypass—The UPS failed or is overloaded.
- 1 Replace battery—The battery failed the 28-day battery test and must be replaced.

For the menus and commands to set these traps, see the user guide that comes with the SNMP module.

Configuring the SNMP subagent in the Avaya Ethernet switch (if used)



Important:

These procedures apply only to a new, Avaya-supplied uninterruptible power supply (UPS) with a Simple Network Management Protocol (SNMP) module. Do not use these procedures to set traps on a UPS that Avaya does not supply.

You must administer the Simple Network Management Protocol (SNMP) subagent in the Avaya Ethernet switch to report alarms to the server when problems occur.

For the SNMP module to properly report alarms, you must configure a unique IP address for the UPS on both the SNMP module and the server. This IP address can be a customer-provided address or the Avaya-provided default address. At a minimum, you must configure the following items:

- 1 The IP address
- 1 The subnet mask
- 1 The gateway IP address
- 1 The trap receiver IP address
- 1 The community string (get, set, trap)

The brand, the model, or the firmware load of the Ethernet switch that Avaya supplies can change without notice. For this reason, this document does not provide specific instructions on how to connect to and configure the SNMP subagent. For more information, see the documentation that comes with the Ethernet switch. Also see the Basic Configuration section of the Quick Start Guide and the documentation CD-ROM that comes with the Ethernet switch for the default user ID, password, and configuration commands.

Note:

For the Ethernet switch to report alarms properly, you must also configure the IP addresses for the Ethernet switches in the servers.

Default IP addresses for the Ethernet switch

For how to administer the SNMP subagent in the Ethernet switches see [Configuring the Ethernet switch](#) on page 33. If the control network is duplicated, perform the same steps for both Ethernet switches.

[Table 5: Default values for a dedicated control network](#) shows the default values for Ethernet switch 1 and Ethernet switch 2 for a dedicated control network.

For non-dedicated control networks, the customer will provide IP addresses

**Important:**

Do not use the IP address of the active server.

Table 5: Default values for a dedicated control network

Parameter	Ethernet switch	Single control network (CNA)	Duplicated control network (CNB)
IP address Subnet mask	1	198.152.254.240 255.255.255.0	198.152.255.240 255.255.255.0
IP address for the trap receiver (server 1)	1	198.152.254.201	198.152.255.201
IP address Subnet mask	2	198.152.254.241 255.255.255.0	198.152.255.241 255.255.255.0
IP address for the trap receiver (server 2)	2	198.152.254.202	198.152.255.202

Preparing to configure the Ethernet switch

Before you configure the Ethernet switch, you must complete the following prerequisites:

- 1 The Ethernet switch power cord is connected to the back of the switch and to the back of a UPS.
 - For a single control network, connect the Ethernet switch 1 for Control Network A (CNA) into UPS 1.
 - For a duplicated control network, connect the Ethernet switch 1 for CNA into UPS 1 and connect the Ethernet switch 2 for Control Network B (CNB) into UPS 2.
- 1 The communication protocol on your computer has the following port settings so that you can use your terminal emulation program:
 - 9600 baud
 - No parity
 - 8 data bits
 - 1 stop bit
 - No flow control

Note:

Avaya Terminal Emulation and HyperTerminal are supported terminal emulation applications.

- 1 If a Network Management System (NMS) is to monitor the Ethernet switch, you coordinated the assignment of community names with the network administrator. If an NMS is not used, you set the community names to unique string values.



SECURITY ALERT:

The Get and Set community name strings are initially configured with the default values of Public and Private, respectively. These community name strings function as passwords for their respective SNMP operation. Avaya recommends that you change these community name strings to something other than the default values. If you leave the defaults in place, a serious security issue can result.

- 1 If the control network is not dedicated, ensure that the 162/udp port for input to server is enabled and the default is disabled. If you do not enable the 162/udp port and disable the default, the server cannot receive the traps from either UPS. See [Enabling firewall settings](#) on page 51.

Configuring the Ethernet switch

Note:

Use the default addresses.

1. Connect the RS-232 serial port of your Services laptop computer to the port labeled Console on the front of Ethernet switch 1 (CNA). Use the flat cable supplied with the Avaya Ethernet switch.
2. Open a VT-100 terminal emulation session on your computer.
3. Set the IP address for the Ethernet switch.
4. Set the subnet mask for the Ethernet switch.
5. Set the gateway IP address for the Ethernet switch.
6. Set the IP address of the trap receiver for the Ethernet switch.
7. Set the SNMP community name string for Get, Set, and Trap. For information about setting these values, see the section on SNMP commands on the documentation CD-ROM that comes with the Avaya Ethernet switch.
8. Use the command `set spantree enabled` to verify that spanning tree is enabled. Note that *enabled* is the default setting.

9. Use the command `set spantree version rapid-spanning-tree` to set the spanning tree version to *rapid-spanning-tree*. Do not use the default.

Note:

This command is available on Avaya Ethernet switches with firmware version 4.0 or later. To use this command, you must update the firmware to this version, if necessary.

For more information on the spanning tree CLI commands, see *Installation and Configuration Guide, Avaya C360* and *Reference Guide, Avaya C360*. These documents are available at the Avaya Support Web site <http://www.avaya.com/support>.

10. If the port networks are IP-PNC, ensure that all appropriate ports on the Ethernet switch are locked to 100 speed and full duplex.
11. When you finish, disconnect your computer from the Ethernet switch.
12. If two Ethernet switches are present for CNA, repeat Steps 1 through 10 for the second switch.
13. If the control network is duplicated, repeat Steps 1 through 11 for each Ethernet switch that remains.

Chapter 3: Communication Manager installation

A new server comes with a blank hard disk drive. Use the bootable software distribution CD-ROM to install the Linux operating system and Communication Manager. On a duplicated system, install the software from the CD onto the hard drive of each server.

This chapter covers the following tasks:

- 1 [Clearing the ARP cache on the laptop](#) on page 35
- 1 [Applying power to the server](#) on page 36
- 1 [Accessing the server](#) on page 36
- 1 [Configuring Telnet for Windows 2000 and Windows XP](#) on page 36
- 1 [Installing Communication Manager](#) on page 37

Clearing the ARP cache on the laptop

Depending on the operating system of your Services laptop computer, you might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. If you enter an IP address and your computer cannot connect, perform the following procedure to clear the cache.

1. On your computer, click **Start** > **Run** to open the Run dialog box.
2. Type **command** and press **Enter** to open an MS-DOS command line window.
3. Type **arp -d 192.11.13.6** and press **Enter** to clear the ARP cache in the laptop.

If the ARP cache does not contain the specified IP address, the system displays the `The specified entry was not found` message. You can ignore this message.

4. Type **exit** and press **Enter** to close the command line window.

Applying power to the server

Note:

In this procedure, the software CD-ROM must be placed into the CD-ROM drive on the server prior to or immediately after you turn on the power to the server.

1. Connect the AC power cord to server 1 and to UPS 1.
2. Press the Power button on the front of the server. Immediately place the Avaya Communication Manager CD-ROM into the CD-ROM drive on the server.

Accessing the server

1. Use a cross-over cable to connect your laptop computer to the Services port on the back of the server. The Services port is labeled 2 and is configured as Eth1.
2. At the command prompt window on your services laptop, type **ping -t 192.11.13.6** and press **Enter**.
The -t causes the ping to repeat continuously. When you get a response, in approximately three minutes, wait an additional 30 seconds before you start a Telnet session to access the information on the CD-ROM.

Configuring Telnet for Windows 2000 and Windows XP

The Microsoft Telnet application might be set to send a carriage return (CR) and a line feed (LF) whenever you press **Enter**. The Communication Manager installation program sees this as two separate key presses. If you are running Windows 2000 or Windows XP, you must correct this setting before you copy the Remaster Program to the hard disk drive.

1. Click **Start > Run** to open the Run dialog box.
2. Type **telnet** and press **Enter** to open a Microsoft Telnet session.
3. Type **unset crlf** and press **Enter**.
4. Type **display** and press **Enter** to verify that you see the message `Line feed mode - Causes return key to send CR.`
5. Type **q** and press **Enter** to exit the telnet session.

Installing Communication Manager

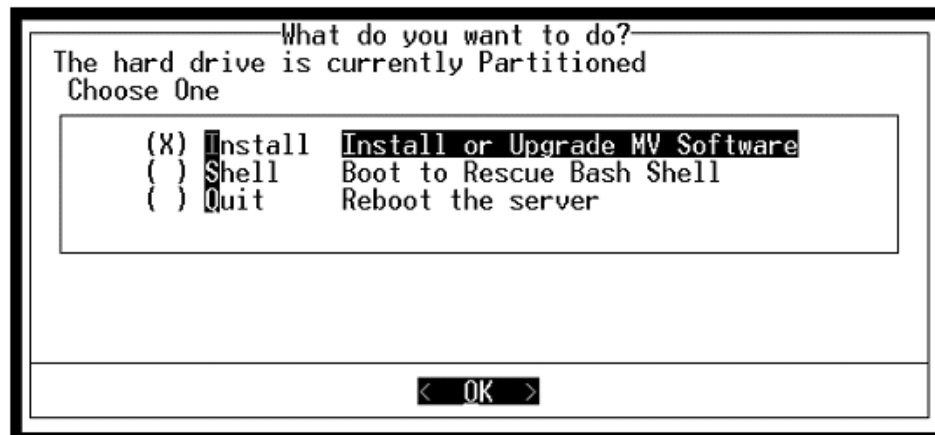
! Important:

When you upgrade a duplicated ESS from an earlier release of Communication Manager to Release 5.2 or later, the duplicated ESS uses the PE Active Server IP address (IP-alias). The upgraded duplicated ESS uses the PE Active Server IP address that is shared by the duplicated ESS pair.

In a situation when the duplicated ESS is upgraded and is running Release 5.2 or later and the main server pair is not yet upgraded and is still running release 5.1.x or prior, the main server has no concept that the duplicated ESS has a PE Active Server IP Address. In this interim state, special consideration must be given to the administration for the duplicated ESS.

Use a Telnet session to access the information on the CD-ROM.

1. On your Services laptop computer, click **Start > Run** to open the Run dialog box.
2. Type `telnet 192.11.13.6` and press **Enter** to view the first screen.



Note:

To navigate on these screens, use the arrow keys to move to an option, and then press the spacebar to select the option. Press **Enter** to submit the information on the screen.

3. Select **Install**, ensure that **<OK>** is highlighted, and press **Enter**.
4. On the **Select Release Version** screen, ensure that the Build line and **<OK>** are highlighted. Then press **Enter**.
5. Press **Enter** to format and partition the hard disk drive and the SSD.
The program starts the installation and displays the progress. This process takes approximately 20 minutes to complete.

Chapter 3: Communication Manager installation

6. When the server is ready to reboot, the drawer of the CD-ROM drive opens. At this time, the CD must be removed from the CD drive. The reboot can take approximately three minutes. The Telnet session drops automatically when the reboot starts.
 - 1 *Using Avaya Enterprise Survivable Server (ESS) guide.*

Chapter 4: Server configuration

After you install the Communication Manager software, you must configure the server.

This section covers the following tasks:

- 1 [Creating a super-user login](#) on page 40
- 1 [Installing the license and authentication files](#) on page 41
- 1 [Configuring the server manually](#) on page 42
- 1 [Running the Avaya Installation Wizard](#) on page 47
- 1 [Verifying the server connection to the customer LAN \(if provided\)](#) on page 47
- 1 [Configuring the modem](#) on page 48
- 1 [Configuring memory for an S8720 Server](#) on page 49
- 1 [Enabling firewall settings](#) on page 51
- 1 [Enabling network time servers](#) on page 51

Note:

Ensure that you have the completed *Electronic Preinstallation Worksheet* (EPW) before you start this process.

Note:

Ensure that your networking and Web browser settings are correct. For more information, see [Configuring the network for Windows 2000 and XP](#) on page 104.

Methods of Configuring a server

The server can be configured using one of the following methods:

1. [Configuring the server manually](#) on page 42 using System Management Interface
2. The Avaya Installation Wizard with the Electronic Pre-installation Worksheet (EPW)
3. The Avaya Installation Wizard interactively

Opening the System Management Interface

Use the System Management Interface to copy license files and authentication files, service packs, and update files from the Services laptop to the server. For how to open the System Management Interface, see [Finding the IP address of the active server](#) on page 101.

Creating a super-user login

Note:

A craft level login can create the super-user login in Release 4.0 or later.

Make sure you have a login name and password that the customer would like for the super-user login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Use the System Management Interface to create a super-user login.

To create a login:

Note:

Make sure the customer can change this login, its password, or its permissions later.

1. On the System Management Interface, click **Administration > Server (Maintenance) > Administrator Accounts**.
2. Select **Add Login**.
3. Select **Privileged Administrator** and click **Submit**.

The **Administrator Accounts -- Add Login: Privileged Administrator** screen appears.

4. In the **Login name** field: Type a login name for the account.
5. In the **Primary group** field: `susers` appears.
6. In the **Additional groups (profile)** field: `prof18` appears (*prof18* is the code for the customer super-user).
7. In the **Linux shell** field: `/bin/bash` appears.
8. In the **Home directory field**: `/var/home/login name` appears (login name is the name you choose in step 4).
9. Skip the **Lock this account** and **Date on which account is disabled**-blank to ignore fields.
10. In the **Select type of authentication section**: Choose **Password**.

Note:

Do not lock the account or set the password to be disabled.

11. In the **Enter key or password field** and the **Re-enter key or password** field: Enter the password.
12. In the **Force password/key change on next login section**: Leave the default to no.
13. Click **Submit**.

Installing the license and authentication files

This section describes the procedure to install the license file and the Avaya authentication file on the active S8700server.

Installing the license file

1. Log on to the System Management Interface and click **Administration > Server (Maintenance) > License File**. The system displays the License File Web page.
2. Do one of the following:
 1. If you have already downloaded the file to this server, select **Install the license file I previously downloaded**.
 1. If you have not downloaded the file to this server, select **Install the license file specified below**, and perform one of the following steps:
 1. In the File Path box, browse to the directory where the license file is located.
 1. In the URL box, enter the location of the license file and in the Proxy Server box, complete the proxy server information.
3. Click **Submit**.

Installing the authentication file

1. **Authentication File**. The system displays the Authentication File Web page.
2. Perform one of the following tasks:
 1. Select **Install the Authentication file I previously downloaded**, if you already downloaded the file to this server.
 1. Select **Install the Authentication file specified below**, and follow these steps:
 - a. In the File Path box, browse to the directory where the authentication file is located.
 - b. Enter the URL where the authentication file is located, and complete the proxy server information.

3. Click **Install**. The system responds with a message that installation of authentication file is successful.

If you get a `filesync failed` message, ignore it.

Configuring the server manually

Note:

If you are configuring the server as a main server, the license files and the authentication files must be downloaded on the server. See [Installing the license and authentication files](#) on page 41.

Setting the date, time, and time zone



Important:

Be sure to set the date, time, and time zone *before* manually configuring the server. Failure to do so may cause network problems.

To set the date, time, and time zone:

1. From the Main Menu, under Server, click **Server Date/Time**.
2. In the **Server Date/Time** window, verify the date and time are correct. If the date and time are incorrect:
 - a. Enter the date in the format *mm/dd/yyyy*.
 - b. Enter the time in 24 hour format (*hh:mm*).
 - c. Enter the time zone.
 - d. Click **Submit**.
 - e. Reboot the server: For more information, see [Rebooting the server](#) on page 42.

Rebooting the server

1. Click **Shutdown Server** under the Server heading.
2. Select **Delayed Shutdown** and **Restart server after shutdown**.
3. Click **Shutdown**.

You will be logged off the server when it reboots. When you are waiting for the system to reboot, enter **ping -t 192.11.13.6** from a command prompt window on your services laptop computer to start a continuous ping command.

System Management Interface configuration screens

The following table shows the Web pages you may need to complete for manual server configuration. For each server configuration (for example, main, LSP, or ESS), the table shows whether that screen must be completed or not.

Table 6: S8700-Series Server configuration web pages

Page	S8700-series Main	S8700-series ESS
Server Role	✓	✓
Set Identities	✓	✓
Configure Interfaces	✓	✓
Configure ESS	✓	✓
Configure Memory (S8720 only)	✓	✓
Configure Switches	✓	✓
Set DNS/DHCP	✓	✓
Set Static Routes	✓	✓
Configure Time Server	✓	✓
Set Modem Interface	✓	✓

The following describes each of the configuration pages:

- 1 **Server Role** — Use the **Specify Server Role** page to assign the server one of the following roles:
 - Main server
 - Enterprise survivable server (ESS)
 - Local survivable server (LSP)

Note:

You must download and install the appropriate license file to complete the server role change.

- 1 **Set Identities** — Use this page to assign Avaya server host names and to assign server functions to a physical Ethernet interface. The options are pre populated with defaults, but should be changed as needed for the customer's configuration. See [Ethernet interface assignments](#) on page 44 for a guide to assigning functions to Ethernet interfaces.
- 1 **Configure Interfaces** — Use this page to enter the IP address, subnet mask, gateway, and speed for the management LAN and control network.
- 1 *(only if Server Role is ESS)* **Configure ESS** — Use this page to configure the server as a primary controller for the system, an Enterprise Survivable Server (ESS). For an ESS use this page to define the memory configuration as Standard or Extra Large. For more information on installing an S8400 as an ESS, see *Using the Avaya Enterprise Survivable Servers (ESS)*(03-300428).
- 1 **Configure LSP** — Use this page to configure the server as a Local Survivable Server (LSP).
- 1 **Configure Memory** — For the S8720 main or ESS server, S8710 ESS server, use this page to configure the server as either standard or extra large. A server that is configured as extra large provides higher capacities.
- 1 **Configure UPS** — Use this page to specify the number of UPS units and the IP address for any Ethernet adjuncts that the Avaya server controls, that are connected to the server over a private LAN.
- 1 **Set DNS/DHCP** — Use this page to enable the different devices (endpoints) in your Avaya call-processing system to communicate over the corporate LAN. Most corporate networks have one or more domain name service (DNS) servers that associate an IP address with the name of a device. When you administer the DNS with the Avaya server names, you can access the servers by name and by IP address over the corporate network.
- 1 **Set Static Routes** — Use this page only if the network administrator instructs you. If the administrator does not specify a particular route for the server to send information over the network, leave the options blank and click **Continue**.
- 1 **Configure Time Server** — Use this page to specify the time source that the Avaya server uses to set the time of day.
- 1 **Set Modem Interface** — Use this page to enable Avaya services or another trouble-tracking service to monitor the Avaya server for alarms. Technical-support representatives can dial in to this interface to fix problems as they occur.

Ethernet interface assignments

Use the following table as a guide for assigning server functions to physical Ethernet interfaces.

Table 7: S8700-series Server Ethernet assignments

	S8710/S8720/ S8730 hardware duplication and dedicated control network	S8720/S8730 software duplication with dedicated control network	S8710/S8720/ S8730 hardware duplication with non-dedicated control network	S8720/S8730 software duplication with non-dedicated control network
Control network A	eth0	eth2	eth0	eth2
Control network B	eth3 (if used)	eth3 (if used)	eth3 (if used)	eth3 (if used)
LAN	eth4	eth4	eth0	eth2
Duplication Link	eth2	eth0	eth2	eth0
Processor Ethernet (PE)	eth0	eth2	eth0	eth2

Note:

For S87xx server software duplication, the duplication link can only be assigned to an Ethernet Interface that supports 1 Gb speed.

Performing the manual configuration

To configure the server using the manual method:

1. Log on to the System Management Interface.
2. From the **Installation** menu, click **Configure Server**.
3. Read and click through the Review Notices to get to the Select Method for Configuring Server page.
4. Select **Configure all services using the wizard** and click **Continue** to get to the Set Server Identities page.
5. Fill in the fields on the Set Identities page and subsequent pages:
 - ┆ Configure Interfaces
 - ┆ Configure ESS
 - ┆ Configure Memory (S8720 only)
 - ┆ Configure Switches
 - ┆ Set DNS/DHCP
 - ┆ Set Static Routes
 - ┆ Configure Time Server

- 1 Set Modem Interface
- 1 Update System

Use your pre-installation planning forms to enter information on these pages. For more information on these pages, see [Configuring the server manually](#) on page 42 or click **Help** at the bottom of each page.

6. When you complete all the fields, click **Continue** on the Update System page. The Update System page displays each configuration task as it completes it and the system displays following message:
`System modifications completed.`

Avaya Installation Wizard

About the Avaya Installation Wizard

Use the Avaya Installation Wizard to:

- 1 Set the date, the time, and the time zone
- 1 Configure the server
- 1 Install the RFA license file

Note:

To install the license file the server does not have to be connected to the reference IPSI. However, you have only 30 minutes before the system checks the serial number on the IPSI. To add another 30 minutes, type `reset system 1` and press **Enter** in a SAT session to restart the Communication Manager software.

- 1 Install the Avaya authentication files
- 1 Install software updates
- 1 Set the product ID
- 1 Set the alarming

The Avaya Installation Wizard cannot be used to configure:

- 1 Extra Large (XL) or Standard Memory Configuration (S8720 only)

Note:

To configure XL or Standard Memory, use the Configure Server in the System Management Interface. For more information see, [Configuring memory for an S8720 Server](#) on page 49.

- 1 Encryption setting for Software Duplication (S8720 or S8730 with Software Duplication)

Note:

To configure Software Duplication, use the Configure Server in the System Management Interface.

To use the Installation Wizard, you can either:

- 1 Import the data from the completed *Electronic Preinstallation Worksheet* (EPW). When the Installation Wizard prompts you to import the Preinstallation Worksheet, click **Import EPW** and browse to the location of the EPW file on your Services laptop computer. The Installation Wizard opens the EPW and uploads the configuration data.
- 1 Type the information manually with the completed EPW as a guide. The Installation Wizard prompts you to enter the configuration data for each step in the Configure Server section.

Running the Avaya Installation Wizard

1. Open a browser on your services laptop computer that is connected to the services port on the front panel of the TN8400 board and type **https://192.11.13.6**
The system displays the Logon page.
2. In the Logon ID box, type **craft** and click **Logon**. The system displays the Password box.
3. In the Password box, type **craft** and click **Logon**. The system displays the Legal Notice page for Communication Manager System Management Interface.
4. From the **Installation** menu, click **Avaya Installation Wizard**.
5. Follow the prompts. For more information use **Help** on each page.



CAUTION:

The license settings for the platform and the port network connectivity (PNC) attributes for the S8700-series Server can be complex. For more information, see [PNC license settings for S8700-series Servers](#) on page 13.



WARNING:

If the time zone is set in the Avaya Installation Wizard (AIW), you must reboot the server after AIW completes.

6. Reboot the server: For more information, see [Rebooting the server](#) on page 42.

Verifying the server connection to the customer LAN (if provided)

1. **Ping**.
2. Select **Host Name Or IP Address** and type the IP address of a computer on the network.

3. Click **Execute Ping**.
4. Verify that the ping was successful and indicates that the server is connected to the customer network.
5. If DNS is administered, type the host name of a computer on the network.
6. Click **Execute Ping**.
7. Verify that the ping was successful and indicates that DNS is working.

If possible, have a customer representative perform the following test from a computer on the network:

1. Click **Start > Run** to open the Run dialog box.
2. Type **command** and click **OK** to open an MS-DOS command window.
3. Type **ping serveripaddress** and press **Enter**, where *serveripaddress* is the IP address of the server.
4. Verify that the ping was successful.
5. If DNS is administered, type **ping servername** and press **Enter**, where *servername* is the host name of the server.
6. Verify that the ping was successful.

Configuring the modem

1. From the **Installation** menu of the System Management Interface, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard page.
3. Select **Configure individual services** and click **Continue**.
4. On the menu on the left, click **Set Modem Interface**.
5. Select **Change Modem Setting** and click **Continue**.
6. In the Extra Modem Initialization Commands window, type the initialization commands that are appropriate for your modem and the country of operation. Click **Help** for help on what to enter.

For example, to change the country code to Japan, type **AT%T19,0,10**.

7. Click **Change**.

The system displays a message that indicates that a modem route was added successfully.

Configuring memory for an S8720 Server

For an S8720 Server, you must select the memory configuration to be used: either Standard or Extra Large. If Hardware Duplication is turned on, administration for the S8720 in an XL configuration is allowed only if the servers are equipped with DAL2 duplication memory cards.

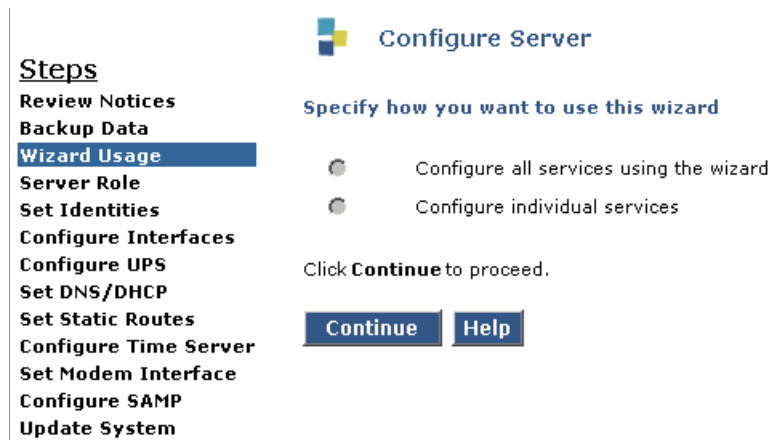
Note:

If the customer chooses to increase the number of VAL circuit packs or the number of Logged-In Agents, the customer will need to get a new License File with increased capacities.

Note:

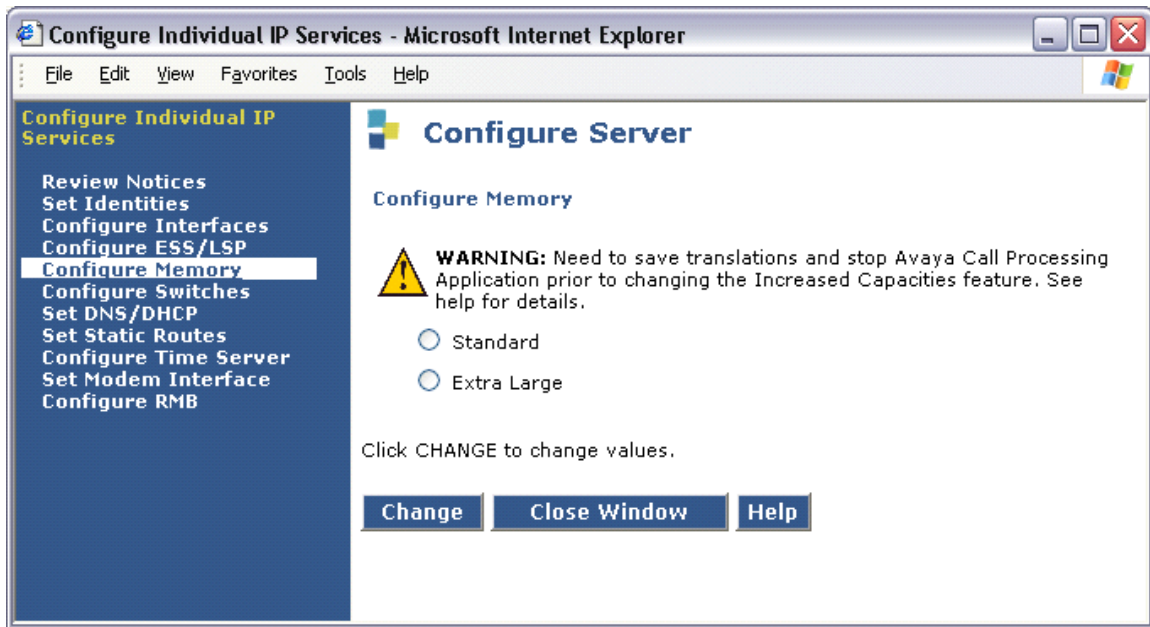
If the main servers are S8720 configured as Extra Large (XL), ESSs and LSPs must be configured as XL. See [Ensuring ESS and LSP compatibility](#) on page 50.

1. Before configuring the memory, stop Communication Manager by running the bash command `stop -acf`.
2. On the System Management Interface, click **Installation > Configure Server**.
3. Click **Continue** until you get to the **Specify how you want to use this wizard** page.



4. Select **Configure individual services** and click **Continue**.
5. On the main menu under Configure Individual IP Services, click
 - 1 **Configure Memory** (if a main server)

1. Configure ESS (if an ESS server)



6. Select either **Standard** or **Extra Large**.
7. Click **Change** to change values.
8. Click **Close Window**.
9. Start Communication Manager by running the bash command `start -ac`.
10. Run the bash command `swversion`.

Ensuring ESS and LSP compatibility

If the main servers are S8730, or if the main servers are S8720 configured as XL, ESSs and LSPs must be configured as XL. S8300B LSPs cannot be configured as XL, and are not compatible with S8730 Servers or with S8720 Servers configured as XL. S8710 ESSs cannot be configured as XL, and are not compatible with S8730 Servers or with S8720 Servers configured as XL.

Enabling firewall settings

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

1. **Firewall.**
2. Scroll down to the snmptrap 162/udp row and select (check) the **Input to Server** box.
The **Output to Server** box can be left as is, either checked or clear.
3. Click **Submit**.

Enabling network time servers



Important:

Avaya strongly recommends that you enable Network Time Protocol (NTP) and configure at least one network time server. If a network time server is not used the Date/Time settings on the server must be reset regularly, at least monthly, using the System Management Interface. The network time strategy is determined by the network administrator.

With NTP, you can specify one, two, or three network time servers to provide the accurate time of day data to the clocks on the servers. The network time servers, in turn, get their source timing from one of several highly accurate time services that are available on the Internet.

To use a network time server, the NTP service must be enabled. The Avaya Installation Wizard prompts you to enable the NTP service. If you do not use the Installation Wizard, use the Configure Server function on the System Management Interface to configure the network time servers.

1. From the **Installation** menu of the System Management Interface, click **Configure Server**.
2. On the Review Notices page and the Backup Up Data page, click **Continue**.
3. On the "Specify how you want to use this wizard" page, select **Configure individual services** and then click **Continue**.
4. In the menu on the left side of the Configure Server page, click **Configure Timer Server**.
5. Enter the NTS information on the **Configure Time Server** screen and click **Change**.
6. On the main menu, under Security, click **Firewall**.
7. In the "Output from Server" column, select **ntp 123/udp**.

Note:

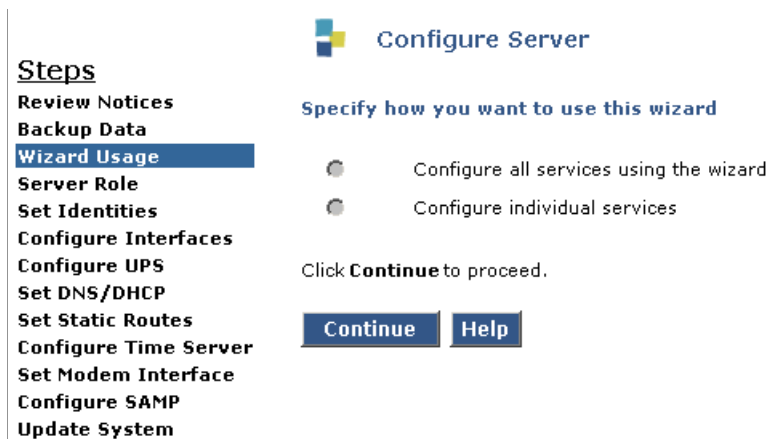
It is not necessary to enable the "Input to Server" ntp service. If this service is already enabled, you do not need to disable it.

When the Avaya Installation Wizard prompts you for information about the network time servers, enter the DNS name or the IP address for the primary network time server and the secondary and the tertiary time servers if any. If you enter a DNS name instead of an IP address for the network time server, you must specify the IP address of the DNS server on the DNS/DHCP Web page. For more information, see [About the Avaya Installation Wizard](#) on page 46.

For more information about NTP, see RFC 958.

Configuring the NIC

1. From the **Installation** menu of System Management Interface, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this Wizard page.



3. Select **Configure Individual Services** and click **Continue**.
4. On the menu on the left, click **Set Identities**
5. Use the drop-down menus to assign the Ethernet port functions. Click **Continue**.
6. Complete the following information for Ethernet 2:
 - 1 IP address
 - 1 Gateway
 - 1 Subnet mask
 - 1 Speed

7. Verify with the network administrator that the LAN hardware supports 802.1q priority tagging. If supported, select **VLAN 802.1q priority tagging**.
8. Click **Change**. The system displays the status of the configuration update.

When the update is complete, the system displays the following message:

Successfully configured ethernet interfaces.

Release the server

Unplug the cross-over cable from the Services port on the back of the server.

Configuring a second server

Use the same procedures that you used to configure the first server. Repeat [Clearing the ARP cache on the laptop](#) on page 35 through [Release the server](#) on page 53 for the second server.

Interchanging servers

Perform an interchange between the two servers to verify that an interchange will work correctly.

Accessing the standby server

To access the standby server:

1. Clear the ARP cache on the laptop if necessary. For more information, see [Clearing the ARP cache on the laptop](#) on page 35 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. If you are not already logged in to the System Management Interface, log in. For more information, see [Accessing the System Management Interface](#) on page 101.

Interchanging servers

To interchange the servers to check capability of the standby server to become the active server:

1. Under Server, click **Interchange Servers**.
2. Verify the settings in the following fields:
 - ┆ **Standby Busied:** no
 - ┆ **Standby Refreshed:** yes
 - ┆ **Standby Shadowing:** on
 - ┆ **Duplication Link:** up
 - ┆ **Control Network health:** X/X/X for both servers, where X is the number of administered IPSI port networks. For more information, see [Chapter 5: IP interface translations](#) on page 57.
3. Click **Interchange**.

The system displays a confirmation message that the interchange has taken place.

This server is now the active server.

To perform another interchange so that the originally active server returns to being the active server:

1. Access the server that is now the standby server. See.
2. Repeat the three steps for [Interchanging servers](#).

Performing an integrity check on the active server

To perform an integrity check on the active server:

1. Log on to the System Management Interface and click **Administration > Server (Maintenance) > Status Summary**.
2. Verify the following:
 - Mode:** Active
 - Server Hardware:** okay
 - Processes:** okay
3. Select **Server > Process Status**.
4. Under Frequency, click **Display Once**.
5. Click **View**.

6. Verify all operations are **UP**.

Note:

Secure-services will be "OFF" if not implemented.
For example, secure-services 0/ 2 OFF.

Chapter 5: IP interface translations

To administer IPSI circuit packs, use a terminal emulation program to issue Communication Manager SAT commands.

For Communication Manager terminal emulation, use a program such as Avaya Native Configuration Manager, Avaya Terminal Emulation, or HyperTerminal.

You also can use Avaya Site Administration to issue SAT commands. To administer some of the features in the latest release of Communication Manager, you must use the latest version of Avaya Site Administration.

Perform these tasks to administer IPSI circuit packs:

- | [Inputting initial system translations](#) on page 57
- | [Adding media gateways](#) on page 58
- | [Enabling the IPSI](#) on page 59
- | [Adding the IPSI to the system](#) on page 60
- | [Enabling IPSI duplication \(duplicated control network only\)](#) on page 61
- | [Setting the alarm activation level](#) on page 61
- | [Saving translations](#) on page 61
- | [Verifying connectivity to the server](#) on page 62
- | [Verifying that the IPSIs are translated](#) on page 62
- | [Upgrading the IPSI firmware version \(if necessary\)](#) on page 62
- | [Enabling control of the IPSIs](#) on page 63
- | [Verifying the license status](#) on page 63

Inputting initial system translations

1. Open a SAT session. See [Accessing the SAT](#) on page 103.
2. Enter translations:
 - If the system translations were prepared offsite, enter the translations and reset the server.
 - If the translations are not available, enter minimal translations to verify connectivity to the port networks.
3. After you enter the translations, type **save translation** and press **Enter** to save the translations to the hard disk drive.

4. Type `reset system 4` and press **Enter** to have the software read the copied translations.

Adding media gateways

Note:

If system translations have been loaded on the server, media gateways do not need to be added to administer the IPSI.

1. Type `add cabinet n` and press **Enter**, where *n* is the cabinet number, for each stack of media gateways that is controlled by one TN2312BP IPSI circuit pack.

A cabinet is defined as a group of up to five G650 Media Gateways that are mounted in a rack and TDM-connected.

2. Fill in the carrier location letter and the carrier type for each media gateway in the cabinet.

add cabinet 1

Page 1 of 1

CABINET

CABINET DESCRIPTION

Cabinet: 1

Cabinet Layout: G650-rack-mount-stack

Cabinet Type: expansion-portnetwork

Number of Portnetworks: 1

Survivable Remote EPN? n

Location: 1

IP Network Region:1

Cabinet Holdover: A-carrier-only

Room: Floor: Building:

CARRIER DESCRIPTION

Carrier	Carrier Type	Number
E	not-used	PN 09
D	not-used	PN 09
C	not-used	PN 09
B	G650-port	PN 09
A	G650-port	PN 09

Enabling the IPSI

1. Type **change system-parameters ipserver-interface** and press **Enter**.
2. On a duplicated server, the system displays the following screen. Verify that the primary control and the secondary control subnetwork addresses are correct.

```

change system-parameters ipserver-interface                               Page 1 of 1
      IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS

SERVER INFORMATION

      Primary Control Subnet Address: 10.13.0.0
      Secondary Control Subnet Address:

OPTIONS

      Switch Identifier: init@svs8730-1-srv1>
      IPSI Control of Port Networks: enabled
      A-side IPSI Preference: enabled
      IPSI Socket Sanity Timeout: 3

QoS PARAMETERS
      802.1p: 6
      DiffServ: 46

```

The control subnetwork addresses typically match the most significant three octets of the IP addresses of the server for the media gateway. The most significant three octets are the first three groups of digits in the IP address. Select the **configure server** command on the System Management Interface to see the IP address of the server.

An asterisk (*) to the right of the **Control Subnet Address** field means that Communication Manager does not have the subnetwork information and the subnetwork address displayed is incorrect.

3. If the information in the **Primary Control Subnet Address** field, the **Secondary Control Subnet Address** field, or both fields is incorrect, use the System Management Interface to change the server configuration to match the Server IP address in **configure server**. Under Server Configuration and Upgrades, click **Configure Server** to change the server configuration. Then return to this procedure.
4. Set the **Switch Identifier** field to the switch ID letter. Acceptable switch ID letters are A through J. A is the default setting.
5. Set the **IPSI Control of Port Networks** field to **enabled**.
6. Press **Enter** to save the changes.

Adding the IPSI to the system

Use the **IP Server Interface Administration - Port Network SAT** screen to add an IPSI. The information on this screen differs, depending on whether the IP addresses of the IPSI are static or assigned automatically through DHCP.

1. Type **add ipserver-interface *PNnumber*** and press **Enter**.
2. For the **Host** field and the **DHCP ID** fields for the primary IPSI and secondary IPSI, if any:
 - i For dynamic addressing, the DHCP server sets the **Host** field and the **DHCP ID** field. Verify that the fields are populated with default data.
 - i For static addressing, in the **Host** field, enter the IP address for the IPSI that is listed in the **Location** field.

```

add ipserver-interface 8                                     Page 1 of 1
      IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 8

IP Control? y          Ignore Connectivity in Server Arbitration? n
Encryption? y

PRIMARY IPSI                                           QoS AND ETHERNET SETTINGS
      DHCP? n          Use System Level Parameter Values? y
                                802.1p: 6
      Location: 5AXX          DiffServ: 46
      Subnet Mask: /24          Auto? y
      IP Address:
      Gateway:

SECONDARY IPSI                                           QoS AND ETHERNET SETTINGS
      DHCP? n          Use System Level Parameter Values? y
                                802.1p: 6
      Location: 5B01          DiffServ: 46
      Subnet Mask: /24          Auto? y
      IP Address:
      Gateway:
  
```

```

add ipserver-interface 8
      IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 3

IP Control? y          Ignore Connectivity in Server Arbitration? n
Encryption? n

PRIMARY IPSI                                           QoS AND ETHERNET SETTINGS
      DHCP? No          Use System Level Parameter Values? y
                                802.1p: 6
      Location: 3A01          DiffServ: 46
      Subnet Mask: /24          Auto? y
      IP Address:
      Gateway:
  
```


3. Set the **IP Control** field to **y**.
4. Verify that all the other fields are populated and submit the screen to save the changes.
5. Repeat this procedure for each port network.

Enabling IPSI duplication (duplicated control network only)

Port networks with duplicated IPSIs have both primary (CNA) and secondary (CNB) IPSI circuit packs. If you disable IPSI duplication, all primary IPSI circuit packs must be active.

Use the System-Parameters Duplication SAT screen to enable IPSI duplication.

1. Enter **change system-parameters duplication**.
2. Enter **y** in the **Enable Operation of IPSI Duplication** field.
3. Submit the screen to save the changes.

Setting the alarm activation level

1. At the SAT, type **change system-parameters maintenance** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, enter **none**, **warning**, **minor**, or **major**, according to the customer request.
3. Submit the screen to save the changes
4. .

Saving translations

To save the translations to the hard disk drive, at the SAT, type **save translation** and press **Enter**.

Verifying connectivity to the server

1. Open the System Management Interface and log on as **craft**.
2. From the Administration menu, click **Server (Maintenance)**.
3. On the left navigation menu, click **Ping** and select **Other server(s), All IPSIs, UPS(s), Ethernet switches** to verify connectivity to these units.
4. Click **Execute Ping**.
5. Verify that all endpoints respond correctly.

Verifying that the IPSIs are translated

Note:

You must be on the active server to use SAT commands.

1. Use SSH to open a SAT session on the server.
2. Type `list ipserver-interface` and press **Enter**.
3. Verify that all ISPI circuit packs are translated.

Upgrading the IPSI firmware version (if necessary)

You might need to upgrade the firmware on some or all the IPSIs. All IPSIs must have the same firmware load.

1. **IPSI Version.**
2. Select **Query All** and click **View**.
3. Verify the firmware release for each IPSI.
4. If an upgrade is required, follow the procedures in *Firmware Download Procedures* at the Download Center on the Avaya Support Web site.

Enabling control of the IPSIs

1. Ensure that the IPSIs have the same, current firmware.
2. For duplicated IPSIs, enable IPSI duplication before you enable IPSI control. See [Enabling IPSI duplication \(duplicated control network only\)](#) on page 61. On the SAT, type **change system-parameters ipserver-interface** and press **Enter**.
3. Ensure the **IPSI Control of Port Networks:** field is set to **enabled**.
4. Submit the screen to save the changes.

Verifying the license status

License File and verify that the license mode is now normal.

Chapter 6: IP interface configuration

This chapter covers the following tasks:

- 1 [Connecting to the IPSIs](#) on page 65
- 1 [IPSI address configuration](#) on page 65
- 1 [Programming the IPSI for static addressing](#) on page 66
- 1 [Setting the VLAN and diffserv parameters](#) on page 68
- 1 [Programming the IPSI for DHCP addressing](#) on page 70

At a minimum, you must program and connect to the reference TN2312BP IP Server Interface (IPSI) so that the system does not enter No License Mode. Once you connect the IPSIs to the control network, the IPSIs might generate an alarm if the firmware is not the most current. The alarm stops automatically once you upgrade the IPSI firmware.

Connecting to the IPSIs

Connect CAT5 cables from the IPSI circuit packs to the dedicated control network or to the customer LAN.

IPSI address configuration

The IPSI circuit pack receives an IP address:

- 1 Statically with static IP addressing, if the control network is nondedicated (public) through the customer network.
- 1 Dynamically with dynamic host configuration protocol (DHCP), if the control network is dedicated (private).

Note:

To program DHCP addressing, you must complete certain sequences within a predetermined time-out interval. Avaya recommends that you read the following procedure completely before you start so that you are familiar with these sequences in advance.

Perform one of the following tasks depending on whether you use static or dynamic addressing:

- 1 [Programming the IPSI for static addressing](#) on page 66
- 1 [Programming the IPSI for DHCP addressing](#) on page 70

Programming the IPSI for static addressing



Important:

If an IPSI is in a port network that is backed up with the Enterprise Survivable Server (ESS) option you must use static addressing for the ESS to provide service to the port network.

You administer the static IP address for the circuit pack directly through the Ethernet port connection on the faceplate (top port). See [Figure 5](#).

Figure 5: Connecting the laptop directly to the IPSI

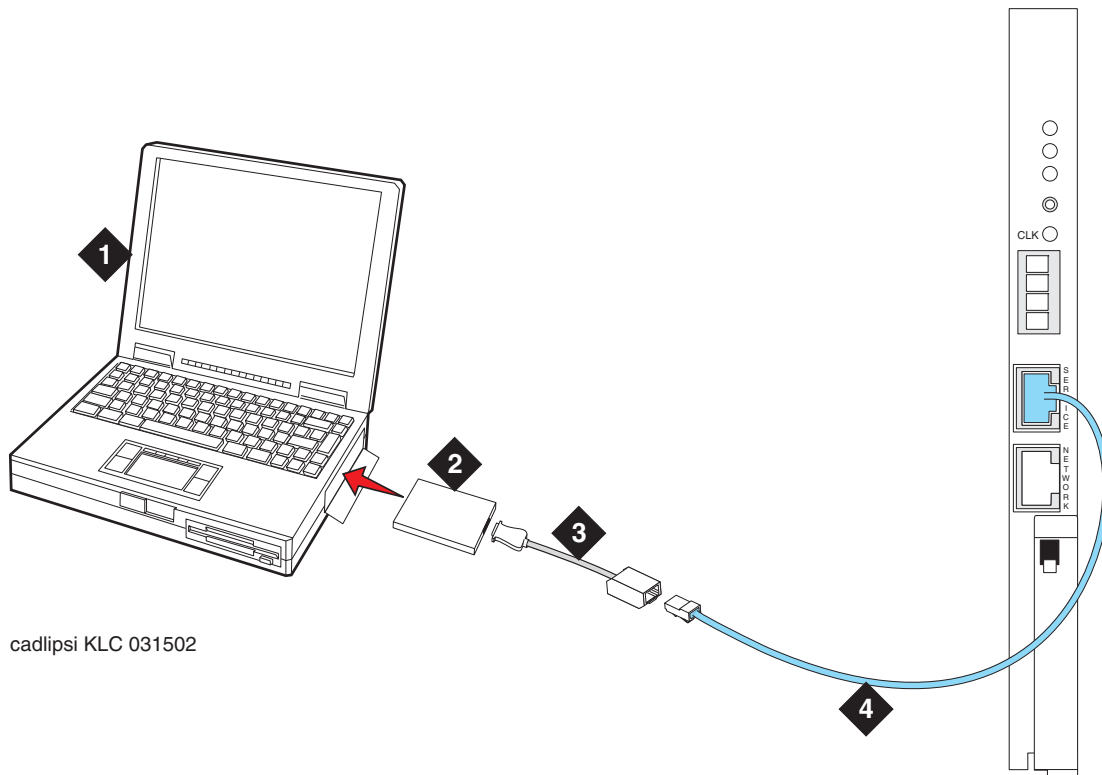


Figure notes:

- | | |
|--|-------------------------------------|
| 1. Services laptop computer | 3. NIC adapter cable (if necessary) |
| 2. PCMCIA Network Interface Card (NIC) | 4. CAT5 crossover cable to IPSI |
-

Note:

Ensure that you have the password before proceeding.

Depending on the operating system on the Services laptop computer, you might need to clear the Address Resolution Protocol (ARP) cache before entering a new IP address. If you enter an IP address and your computer cannot connect, try clearing the cache.

1. On your laptop computer, click **Start > Run** to open the Run dialog box.
2. Type **command** and click **OK** to open a MS-DOS Command Line window.
3. Clear the Address Resolution Protocol (ARP) cache in the laptop.
4. To log into the IPSI, use SSH and the IP address **192.11.13.6**.

For information on how to use SSH, see [Accessing the command line interface of the server with SSH](#) on page 95.

Note:

While connected to the IPSI, type **help** or **?** to obtain online help. Most commands have two or three letter abbreviations.

5. Type **ipsilogin** and press **Enter**.

Note:

The *craft* login used on the IPSI has a different password from the *craft* login used on the servers.

6. Log in as **craft**.

Prompt = [IPADMIN]:

7. Type **show control interface** and press **Enter** and then type **show port 1** and press **Enter** to see the current control interface settings.

8. To set the control interface, type `set control interface ipaddr netmask` and press **Enter**, where *ipaddr* is the customer-provided IP address and *netmask* is the customer provided subnet mask.

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

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

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

[IPADMIN]: show control interface

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

[IPADMIN]: █
```

9. Type `quit` and press **Enter** to save the changes and exit the IPSI session.
10. Log back in to the IPSI using SSH.
11. Type `show control interface` and press **Enter**.
The system displays IP address, subnet mask, and default gateway information.
Verify that the proper information was entered.
12. If a default gateway is used, enter the gateway IP address with
`set control gateway gatewayaddr`, where *gatewayaddr* is the customer-provided IP address for their gateway.
13. Type `quit` and press **Enter** to save the changes and exit the IPSI session.
14. Log back in to the IPSI using SSH.
15. Use `show control interface` to verify the administration.
16. Type `exit` and press **Enter**.

Setting the VLAN and diffserv parameters

1. Connect to the IPSI and log in as `craft`.
2. To display the quality of service values, type `show qos` and press **Enter**.

3. Use the **set** commands in the list below to set the VLAN, diffserv, and port parameters. If the customer does not specify different values, use these recommended values.

Note:

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



Important:

The settings for these parameters on the IPSIs must be consistent with the settings on the servers and other network devices such as Ethernet switches.

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

4. Type **show qos** and press **Enter** to check the administered values.
5. Type **reset** and press **Enter** to capture the updated parameter values.
The reset terminates the administration session and automatically logs you out.
6. Log in again and use the **show qos** command to ensure that the parameter settings are correct.
7. Disconnect the laptop from the IPSIfaceplate.
8. Check the LED on the IPSIfaceplate. Verify that the display shows the letters I and P and a filled-in V at the bottom. (See [Figure 6](#)).

Figure 6: IPSI LED display for static address

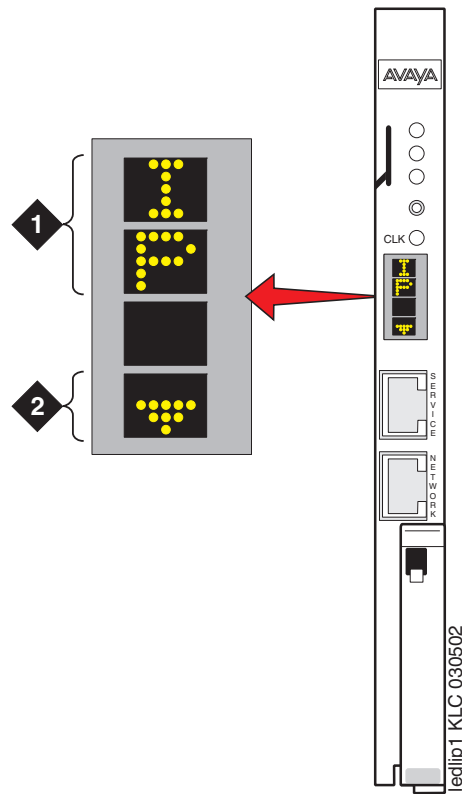


Figure notes:

1. IPSI has a static IP address
2. IPSI has connectivity and an IP address

Note:

Clear the ARP cache on the laptop before connecting to another IPSI. If you do not clear the cache, the laptop appears to stop and does not connect to the next IPSI.

9. Repeat this procedure for each IPSI circuit pack.

Programming the IPSI for DHCP addressing



Important:

If an IPSI is in a port network that is backed up with the Enterprise Survivable Server (ESS) option you must use static addressing for the ESS to provide service to the port network.

For the TN2312BP IPSI circuit packs to receive IP addresses dynamically, you first must assign the switch ID and cabinet number to each IPSI circuit pack. The switch ID is a single letter, A through J. The cabinet number is a 2-digit number, 01 through 64. For G650 Media Gateways, a cabinet is defined as one or more media gateways connected by a TDM cable. This cabinet configuration is called a G650-rack-mount-stack.

Note:

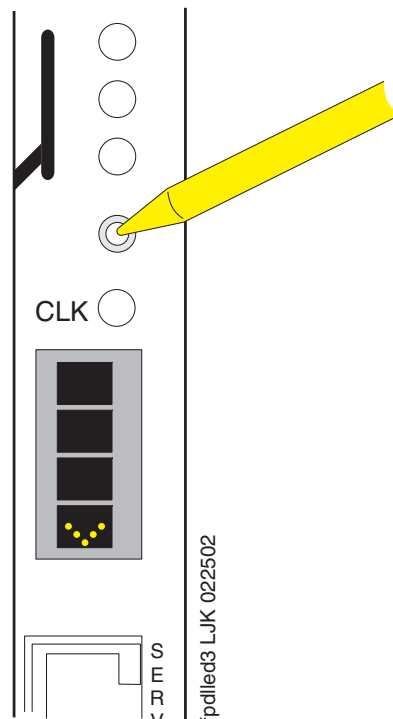
In the following procedure, you must start step 2 within 5 seconds after inserting the circuit pack.

1. Fully insert the TN2312BP IPSI circuit pack. If necessary, reseal the circuit pack to start the programming sequence.

Note:

For the following step, do not use a graphite pencil.

2. Insert a pen, golf tee, or similar object into the recessed push button switch.



Note:

If you pass the letter or number that you want, you have two options. You can cycle through all the letters or numbers to get to the one you want. Or, you can reinsert, or reseal, the circuit pack and start again.

Note:

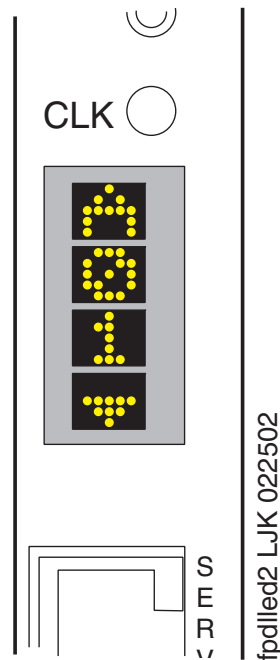
If you have only one system, the default switch ID is A. The second system is B and so on. The switch ID is *not* the media gateway or carrier letter.

3. While the display characters are flashing, press the button until the switch ID, A through J, shows on the top character of the LED display. When the correct letter shows, stop. The letter flashes a few times, or 5 seconds, then stops. The next character down starts to flash. This is the first digit of the cabinet number.

Note:

The number to program is the cabinet number, not the port network number. If you have more than one IPSI in a cabinet, they all have the same cabinet number.

4. While the first digit of the number is flashing, press the button until the correct tens digit, 0 through 6, for the cabinet number shows on the display. When the correct digit appears, stop. The digit flashes for about 5 seconds, then stops. Then the second digit starts flashing.
5. While the second digit is flashing, press the button until the correct units digit, 0 through 9, for the cabinet number shows on the display. When the correct digit shows, stop. The digit flashes for about 5 seconds, then stops.
6. All segments of the display go dark for one second. Then, the Switch ID and media gateway stack number shows in the top three characters of the LED display. A ▽ is shown in the fourth or bottom character. When the DHCP server assigns an address to the IPSI, the center of the ▽ fills in. The filled in ▽ looks like the bottom half of a diamond.



For a duplicated control network, repeat these steps for the second IPSI in the cabinet.

Chapter 7: Postinstallation administration

This section covers the following tasks:

- | [Verifying translations](#) on page 73
- | [Setting rules for daylight savings time](#) on page 74
- | [Setting locations \(if necessary\)](#) on page 75
- | [Verifying the date and the time \(main server only\)](#) on page 76
- | [Clearing and resolving alarms](#) on page 77
- | [Enabling and disabling the Ethernet switch ports](#) on page 77
- | [Backing up files to the compact flash media](#) on page 80
- | [Enabling alarms to INADS by way of a modem](#) on page 79
- | [Enabling alarms to INADS by way of the SNMP module](#) on page 80
- | [Before leaving the site](#) on page 81

Verifying translations

1. Open a SAT session on the server.
2. To view all the administered circuit packs in the system, type `list configuration all` and press **Enter**.
3. To verify the location of the IPSI circuit packs, type `list ipserver-interface` and press **Enter**.

For more information, see your planning documents and check the administration status on the following items:

- | `list station`
- | `list trunk-group`
- | `list hunt-group`

Setting rules for daylight savings time

Use the System Management Interface to set the date, time, and time zone on the server. You must use SAT commands to set the rules for daylight savings time.

Note:

The default setting of the daylight-savings-rules SAT screen reflect the US and Canada rules effective in 2007.

1. Type **change daylight-savings-rules** and press **Enter**.
2. In the **Change Day, Month, Date, Time**, and **Increment** columns, type the appropriate start and stop information for each rule. For example, **1:00** in the **Increment** field means to move the clock forward or back by one hour at the transition point.

You can set up to 15 customized daylight savings time rules. If you have media gateways in several different time zones, you can set up rules for these media gateways on a per-location basis. A daylight savings time rule specifies the exact time when you want to transition to and from daylight savings time. The rule also specifies the increment at which to make the transitions.

Note:

The default daylight savings rule is **0**, which means that no daylight savings transition occurs. You can change any rule except rule 0. You cannot delete a daylight savings rule if the rule is in use on either the Locations screen or the Date and Time screens.

3. When you finish, submit the screen to save the changes.

Setting locations (if necessary)

After you set the rules for daylight savings time, you must set the locations for all port networks. Port networks can be in different time zones. Use SAT commands to set the locations for the port networks.

1. Type **change locations** and press **Enter**.

change locations		LOCATIONS		Page	1 of	5
ARS Prefix 1 Required For 10-Digit NANP Calls? y						
Number	Name	Timezone Offset	Daylight-Savings Rule	Number	Plan	Area Code
1	Main	+ 00:00	0			
2	CA	- 02:00	0			
3		:				
4		:				
5		:				
6		:				
7		:				
8		:				
9		:				
10		:				
11		:				

2. In the ARS Prefix 1 Required for 10-Digit NANP Calls? field, type **y**. The system displays the location information.
3. Click **Submit** to save the changes.

Note:

The location of a port network is defined on the **Cabinet** SAT screen (**change cabinet x**). The location of a network region is defined on the **ip-network-region** SAT screen (**change ip-network-region x**). The location of an H.248 media gateway is defined on the **change media-gateway** SAT screen (**change media-gateway x**). The **Location** field in the **ip-network-region** SAT screen is part of the association to the daylight-savings-rule by which a IP phone behaves.

Verifying the date and the time (main server only)

Use SAT commands to verify the date and time.


1. Type **display time** and press **Enter**.

```
display time                                     Page 1 of 1
                                     DATE AND TIME

DATE
    Day of the Week: Friday           Month: June
    Day of the Month: 9               Year: 2006

TIME
    Hour: 14 Minute: 19 Second: 36   Type: Standard
    Daylight Savings Rule: 0

WARNING: Changing the date or time may impact BCMS, CDR, SCHEDULED
```

2. Verify that the date and the time of day are correct.
If the date and the time of day are correct, go to 5.
If the date and time of day are not correct, proceed to step 3.
 3. Verify connectivity to any administered Network Time Server:
 - a. On the System Management Interface, from the **Administration** menu, click **Server (Maintenance)**.
 - b. On the left navigation panel, click **Network Time Sync**. The Network Time Sync screen confirms synchronization to any administered Network Time Server.
 - c. Resolve any connection or administration issues related to the Network Time Server. If the Network Time Server is not administered:
 1. On the left navigation menu, click **Server Date/Time**.
 2. Set the correct date and the correct time. Verify that the time zone is correct.
-  **Important:**
If you change the time zone, you must reboot the server. For more information, [Rebooting the server](#) on page 42.
4. Repeat this procedure, beginning with step 1.
 5. Verify that the Daylight Savings Rule field is correct.
 - i 0 if this server is in a location that does not use daylight savings time

- I 1-15 use an administered rule. The rule is administered using the SAT command daylight-savings-rules. For more information on the daylight-savings-rules, see [Setting rules for daylight savings time](#) on page 74.

Note:

The daylight savings rule setting on this screen is the rule that is utilized by the Communication Manager software. Additional daylight savings rules can be implemented for the specific locations of hardware supported by the Communication Manager software. For more information, see [Setting locations \(if necessary\)](#) on page 75.

Clearing and resolving alarms

1. **Current Alarms.**

You can resolve alarms on the *active* server only.

2. Select the server alarms to clear and click **Clear**.

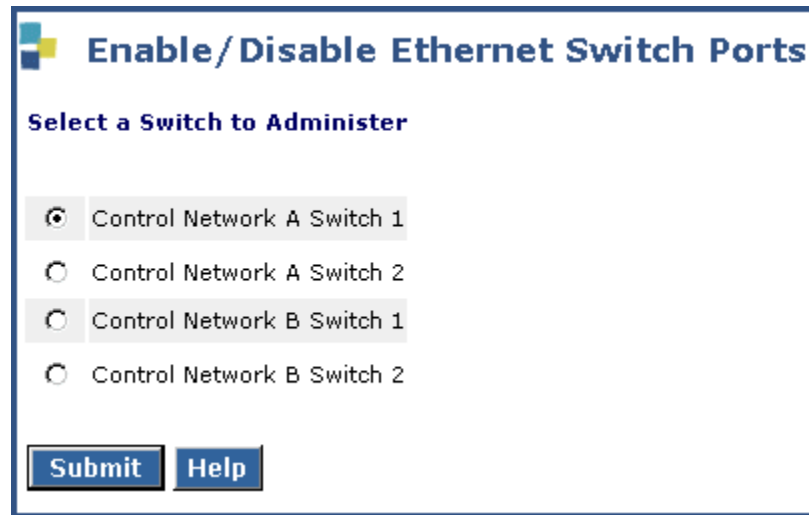
Note:

Use SAT commands or other standard troubleshooting procedures, to resolve any major alarms.

Enabling and disabling the Ethernet switch ports

You might want to disable unused ports on the Avaya Ethernet switch, if used.

1. To select an Ethernet switch to administer, under Security, click **Ethernet Switch Ports**.



The screenshot shows a web interface titled "Enable/Disable Ethernet Switch Ports". Below the title is a section labeled "Select a Switch to Administer". This section contains four radio button options: "Control Network A Switch 1" (which is selected), "Control Network A Switch 2", "Control Network B Switch 1", and "Control Network B Switch 2". At the bottom of the form are two buttons: "Submit" and "Help".

2. Select the switch you want to administer and click **Submit**.

Enable/Disable Ports for Control Network A Switch 1

Port	Enable	Disable
1	<input checked="" type="radio"/>	<input type="radio"/>
2	<input checked="" type="radio"/>	<input type="radio"/>
3	<input checked="" type="radio"/>	<input type="radio"/>
4	<input checked="" type="radio"/>	<input type="radio"/>
5	<input checked="" type="radio"/>	<input type="radio"/>
6	<input checked="" type="radio"/>	<input type="radio"/>
7	<input checked="" type="radio"/>	<input type="radio"/>
8	<input checked="" type="radio"/>	<input type="radio"/>
9	<input checked="" type="radio"/>	<input type="radio"/>
10	<input checked="" type="radio"/>	<input type="radio"/>
21	<input checked="" type="radio"/>	<input type="radio"/>
22	<input checked="" type="radio"/>	<input type="radio"/>
23	<input checked="" type="radio"/>	<input type="radio"/>
24	<input checked="" type="radio"/>	<input type="radio"/>
25	<input checked="" type="radio"/>	<input type="radio"/>
26	<input checked="" type="radio"/>	<input type="radio"/>

Submit Changes

Help

3. Locate the ports that you want to disable and select **Disable** in that row.
4. Click **Submit Changes**.

Enabling alarms to INADS by way of a modem

Note:

Enable alarms on both servers.

1. Start an SSH session on the server.
2. Type `almenable -d b` and press **Enter**.

3. To verify that the alarms are enabled, type `almenable` and press **Enter**.

Enabling alarms to INADS by way of the SNMP module

Note:

Perform this procedure only if the installation includes a Secure Service Gateway (SSG).

To enable alarms on the servers:

1. Start an SSH session on the server.
2. Type `almsnmpconf -d ipaddress -c communityname` and press **Enter**, where *ipaddress* is the trap receiver address for the SSG device and *communityname* is the community string name that the SSG device requires.
3. Type `almsnmpconf` and press **Enter** and verify that the correct information is entered.
4. Type `almenable -s y` and press **Enter**.
5. Type `almenable` and press **Enter** and verify that alarm origination is enabled on the SNMP module. If used, also verify that alarm origination by way of a modem is still enabled.
6. Log off.

Backing up files to the compact flash media

Note:

Avaya requires the use of industrial grade compact flash media.

1. Connect the compact flash drive to one of the USB ports on the back of the server.
2. Insert the compact flash media into the top right slot of the drive.
3. **Backup Now.**
4. Select all applicable data sets.
5. To back up the data onto the compact flash media, select **Local PC Card**.

To format a new media card, also select **Format PC Flash**.

Note:

You must format the compact flash media before the first use only.

6. Click **Start Backup**. The system displays a message when the format is completed, which takes approximately 10 seconds.



CAUTION:

If you click **Start Backup** without media in the compact flash drive, you cause a system error. In this case, repeat the steps beginning with Step 1.



WARNING:

Do not remove the Compact Flash card when the Compact Flash in use LED (yellow) is ON. Doing so may corrupt the data on the Compact Flash card.

7. To view the status of the backup, click **Backup Status**.

Before leaving the site

- 1 Provide the default LAN security settings to the customer.
- 1 Ensure that the customer knows that remote access to the server is available only if the following services are enabled on the Firewall screen:
 - **SSH** must be enabled
 - **https** must be enabled to access the System Management Interface
 - **def-sat** must be enabled to access the SAT commands
 - **162/udp** must be enabled to receive SNMP traps from the UPS and the Avaya Ethernet switch

Chapter 8: Installation verification

This chapter provides the following information about how to verify the server installation and configuration:

- 1 Testing the IPSI circuit packs
- 1 Testing the license file
- 1 Checking LED status indicators
 - Servers
 - Avaya Ethernet switches
 - Uninterruptible power supplies (UPSs)
 - Circuit packs

Testing the IPSI circuit pack

The following steps test the clock and packet interface components within the TN2312BP IPSI circuit pack.

Note:

With duplicated servers, use the active server.

1. In a SAT command line, type `test ipserver-interface UUC` and press **Enter**, where *UUC* is the cabinet and the carrier in which the circuit pack is located.
2. Verify that the Test Results screen shows PASS in the Results column.

Testing the license file



Important:

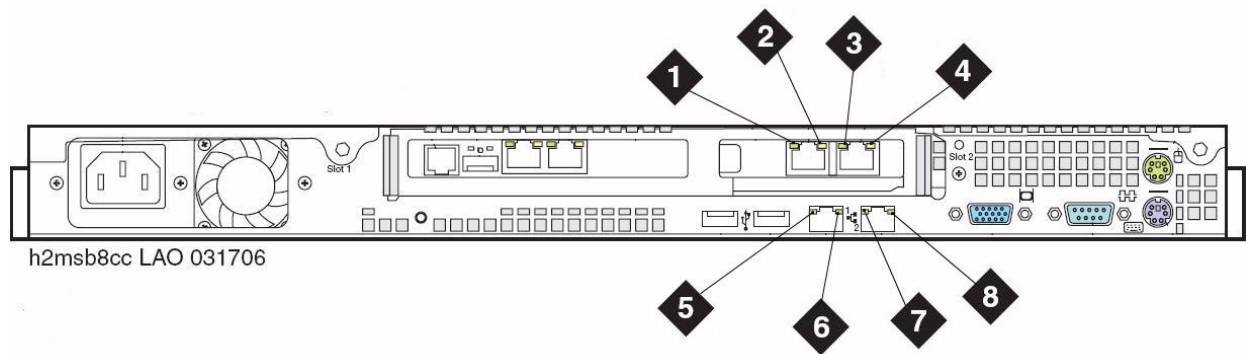
Wait at least 30 minutes after you install the Communication Manager license before you run this test.

Note:

With duplicated servers, use the active server.

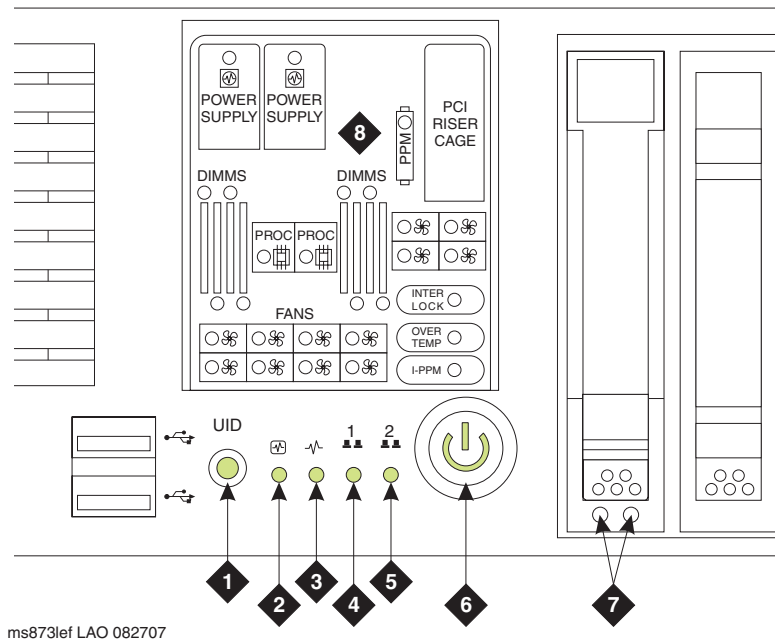
1. On a SAT command line, type `test license` and press **Enter**.
2. Verify that the Test Results screen shows PASS in the Results column.

Figure 7:



S8730 LEDs

[Figure 8: LEDs on the front panel of the S8730 Server](#) on page 85 and [Figure 9: LEDs on the back panel of the S8730 Server](#) on page 86 show the LEDs on the S8730 Server.

Figure 8: LEDs on the front panel of the S8730 Server
**Figure notes:**

- | | |
|-------------------------------|--|
| 1. Active/standby LED | 6. Power on/standby button/system power. Amber means system shut down, but power still applied. Green means system on. To turn off the power, press and hold the Power button for several seconds. |
| 2. Internal health | 7. Hard Drive LEDs |
| 3. External health | 8. System Insight Display LEDs, which represent the system board layout. |
| 4. NIC 1 (Eth0) link/activity | |
| 5. NIC 2 (Eth1) link/activity | |

Note:

The Active/Standby LED, which is labeled as 1 in [Figure 8](#), is on a push button. When pushed, this button has no effect other than to turn off the LED momentarily. The LED returns to the normal state within a few seconds after the button is pushed.

Figure 9: LEDs on the back panel of the S8730 Server

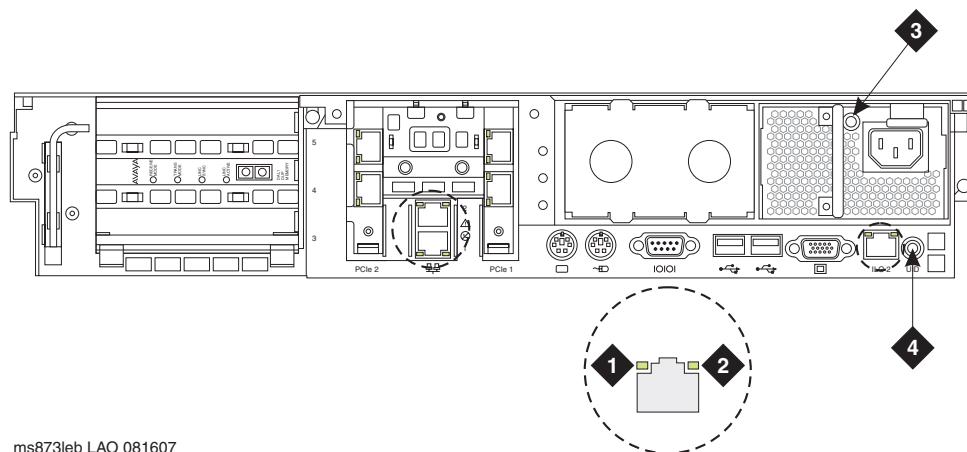


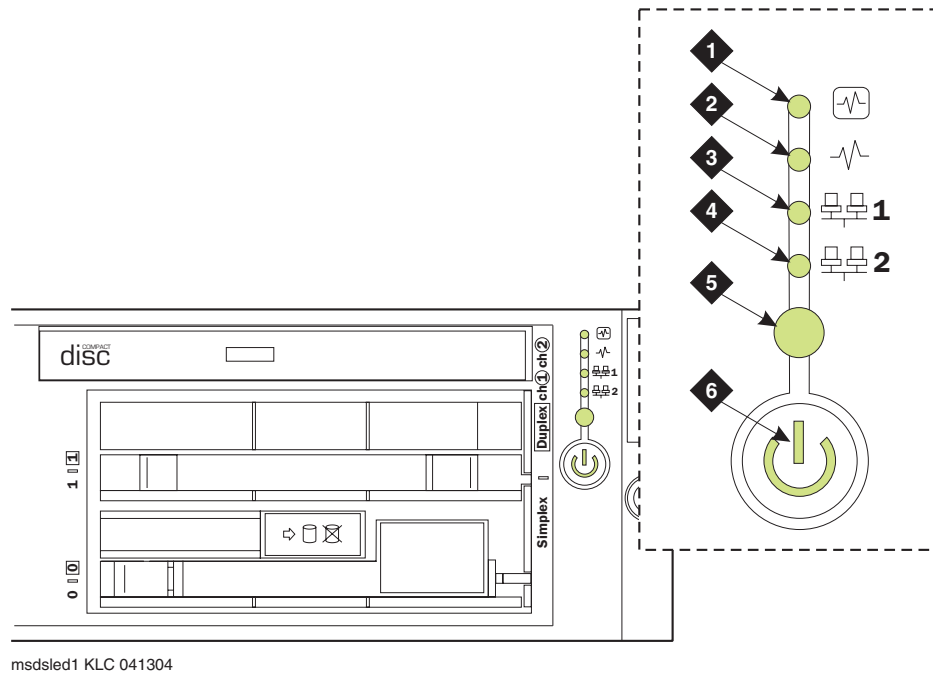
Figure notes:

1. NIC activity LED
2. NIC link LED
3. Power supply LED
4. Active/standby LED. Indicates active when on steady or standby mode when blinking (blue). This LED duplicates the Active/Standby LED on the front panel.

S8710 and S8720 LEDs

[Figure 8: LEDs on the front panel of the S8730 Server](#) on page 85 and [Figure 9: LEDs on the back panel of the S8730 Server](#) on page 86 show the LEDs on the S8710 and the S8720 Servers.

You cannot test the LEDs on the S8710 Server.

Figure 10: LEDs on the front panel of the S8710 and the S8720 Servers
**Figure notes:**

- | | |
|---------------------------------------|---|
| 1. Internal health | 4. NIC 2 (Eth1) link/activity (green) |
| 2. Power supply | 5. Indicates active when on steady or standby mode when blinking (blue) |
| 3. NIC 1 (Eth0) link/activity (green) | 6. Power on/standby button/system power. Amber indicates power to the chassis is on but the server is off. Green indicates power is on and the system is running. To turn off the power, press and hold the Power button for several seconds. |
-

Note:

The Active/Standby LED, which is labeled as 5 in [Figure 10](#), is on a push button. When pushed, this button has no effect other than to turn off the LED momentarily. The LED returns to the normal state within a few seconds after the button is pushed.

Figure 11: LEDs on the back panel of the S8710 and the S8720 Servers

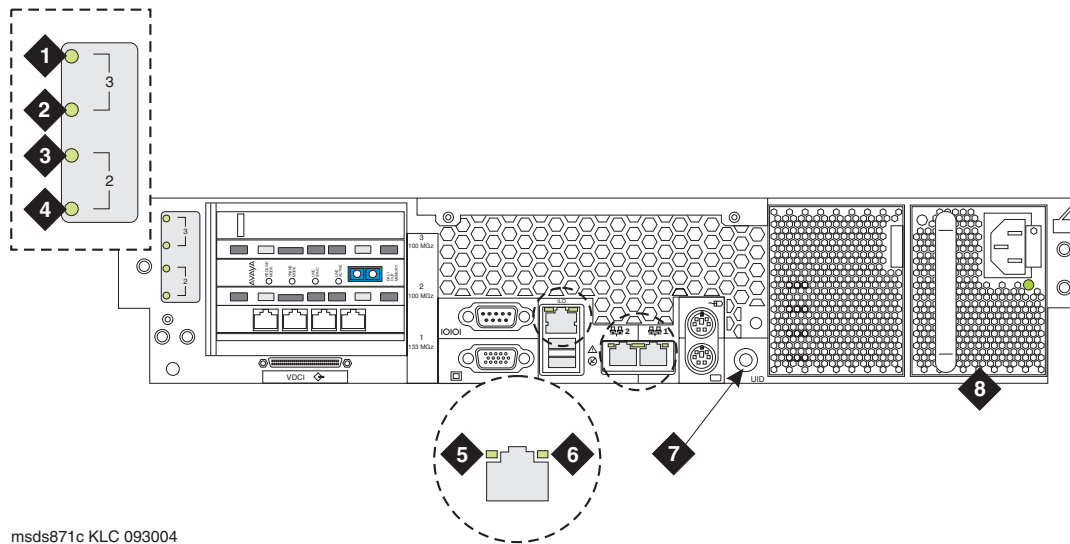


Figure notes:

- | | |
|---|---|
| 1. Not used | 5. RJ45 link (green) |
| 2. Not used | 6. RJ45 link (green) |
| 3. For hardware duplication mode on the S8710, DAL2 fault (amber) | 7. Indicates active when on steady or standby mode when blinking (blue) |
| 4. For hardware duplication mode on the S8710, DAL2 power (green) | This LED duplicates the Active/Standby LED on the front panel. |
| | 8. Power supply (green) |

Additional server LED information

For more information on server LEDs, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

- (When S8400 is deployed as an ESS). The S8400 ESS raises a major alarm when it becomes active. The raising of this alarm also lights the red alarm LED on the faceplate of the S8400 circuit pack.

Avaya C360 Ethernet switch LEDs

The C360 series converged, stackable, Ethernet switches include:

- 1 C363T: 24-port
- 1 C363T-PWR: 24-port power over Ethernet (PoE)
- 1 C364T: 48-port
- 1 C364T-PWR: 48-port PoE

The front panel of the C360-Series switches has:

- 1 One port LED that is associated with each port
- 1 Three system status LEDs
- 1 Seven port function LEDs

The C363T-PWR and the C364T-PWR switches have an additional PoE LED. The port function LEDs are selectable with a set of two left/right buttons. The port LEDs display the status of the selected function for each port.

For more information about the on/off and blinking states of the LEDs, see the documentation for the Ethernet switch.

System and port function LEDs on C360 Avaya Ethernet switches

LED Name	Description
System LEDs	
PWR	Power status
SYS	System status
ROUT	Routing mode
Port Function LEDs	
LNK	Link status
COL	Collision status
Tx	Transmit to line
Rx	Receive from line
FDX	Full duplex mode
Hspd	High-speed mode
LAG	Link aggregation group for trunking
PoE (PWR versions only)	Power over Ethernet status

UPS LEDs

The UPS LEDs flash briefly after the UPS is plugged in. The normal mode LED flashes after a self-test to indicate that the UPS is in standby mode.

For more information, see the UPS user guide for the Powerware UPS.

Figure 12: LEDs on the Powerware 9125 UPS

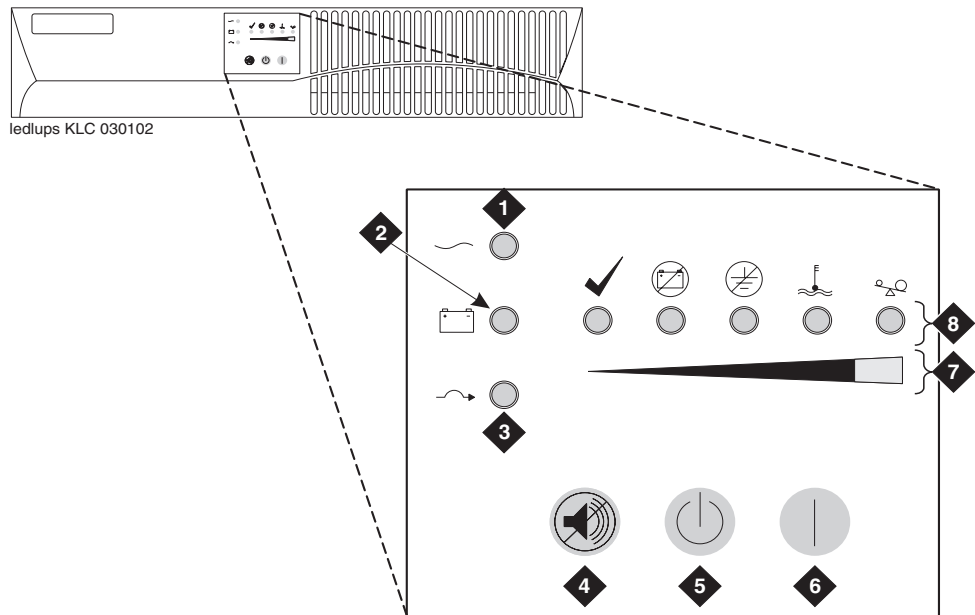


Figure notes:

- | | |
|----------------------------|-------------------------|
| 1. Normal mode indicator | 5. Off button |
| 2. Battery mode indicator | 6. On button |
| 3. Bypass mode indicator | 7. Bar graph indicators |
| 4. Test/Alarm reset button | 8. Alarm indicators |

TN2312BP IPSI LEDs

TN2312BP IP Server Interface (IPSI) circuit pack LEDs include:

- 1 Standard LEDs and connector slots
- 1 A programmable LED display, which indicates:
 - The type of IPSI IP address. For a dynamic address, the display shows media gateway the location of the media gateway. For a static address, the display shows
I P. ([Figure 14: IPSI LED display for a static IP address](#) on page 93)
 - 1 Connectivity . If SIPI has connectivity and an IP, the LED panel shows a solid downward pointing triangle (see [Figure 14](#)).

For more information on troubleshooting the configuration of the server hardware, see [Appendix B: Installation troubleshooting](#) on page 107.

Figure 13: TN2312BP IPSI circuit pack faceplate

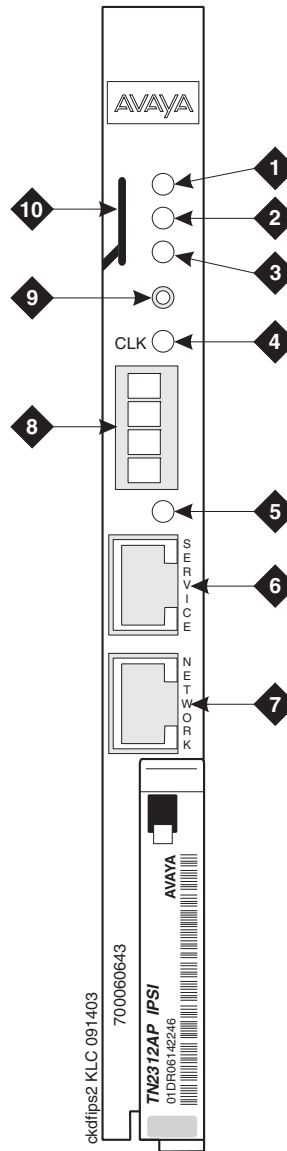
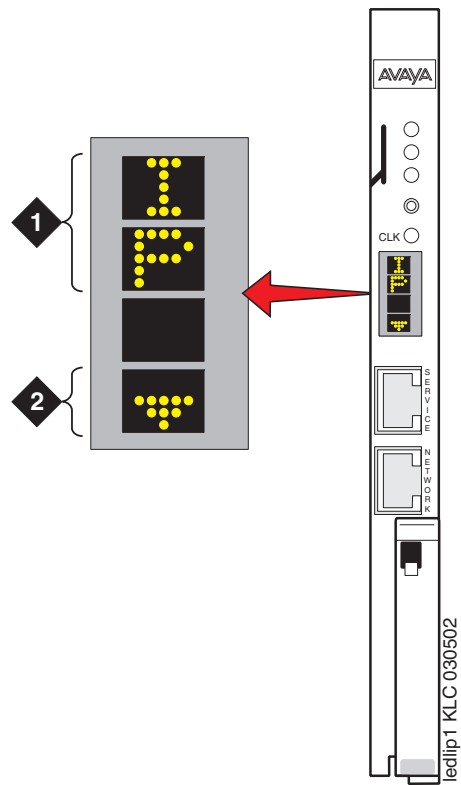


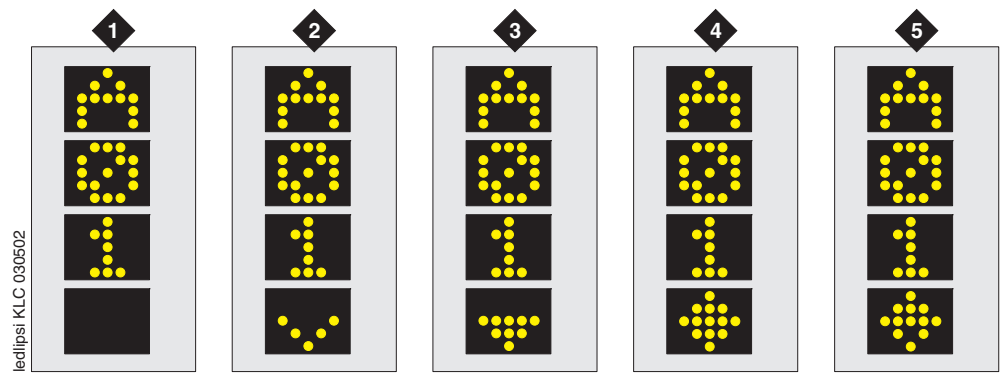
Figure notes:

- | | |
|---|------------------------------------|
| 1. Red LED (ON indicates power up/failure) | 6. Services RJ45 connector |
| 2. Green LED (ON indicates circuit pack in use) | 7. Network control RJ45 connector |
| 3. Amber LED (ON indicates maintenance diagnostics/testing) | 8. Four-character LED display |
| 4. Yellow LED (tone clock status) | 9. Pushbutton switch |
| 5. Emergency transfer LED | 10. Slot for the maintenance cable |

Figure 14: IPSI LED display for a static IP address**Figure notes:**

1. The IPSI has a static IP address.
 2. The IPSI has connectivity and an IP address.
-

Figure 15: IPSI LED display indicating connectivity status for a DHCP IP address



Connectivity status	1	2	3	4	5
The IPSI is connected to a server.	No	Yes	Yes	Yes	Yes
The IPSI has an IP address.	No	No	Yes	Yes	No
The Services laptop computer is connected to the IPSI services port.	No	No	No	Yes	Yes

Appendix A: Server access

Use a personal computer or a Services laptop computer that is equipped with a network interface card (NIC), a terminal emulation program, and a Web browser to access a server for initial configuration, aftermarket additions, and continuing maintenance.

You can access the server:

- 1 Directly
- 1 Remotely over the customer network
- 1 Remotely over a modem (for Avaya maintenance access only)

Steps to access a server include:

- 1 [Connecting to the server directly](#) on page 97
- 1 [Connecting to the server remotely over the network](#) on page 100
- 1 [Connecting to the server remotely over a modem](#) on page 100
- 1 [Logins for Avaya technicians and Business Partners](#) on page 103
- 1 [Configuring the network for Windows 2000 and XP](#) on page 104

Accessing the command line interface of the server with SSH

The procedure in this section shows how to use SSH to log on to the server from a Services laptop computer. SSH is the recommended method for server access. To use this procedure with a cross-over cable connection from the computer to the Services port, you must configure the computer for the network connection.

To use SSH, a third-party SSH client must be installed on your computer. PuTTY is one such client. You can download PuTTY from <http://www.putty.nl/download.html>. The following procedure describes, as an example of SSH access, how to log on to the server command line with PuTTY.

Note:

Many Avaya products support access with SSH. However, Avaya does not provide support for third-party clients that are used for SSH access. Problems with an SSH client, including PuTTY, are the responsibility of the user or the SSH client vendor.

Use the following instructions if you are using PuTTY as the SSH client.

Appendix A: Server access

1. On your computer, click the **PuTTY** desktop link or click **Start > Programs > PuTTY > PuTTY**.

The system displays the PuTTY Configuration window with the Session dialog box open.

2. In the Host Name or IP address field, type **192.11.13.6** if you want to connect to the Services port. For access over the LAN or WAN, type the IP address or the host name of the server.
3. In the Port field, type **22**.
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection > SSH**.
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 also 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 **Backspace key** area, select **Control-H**.

This activates the backspace key while you are using the SAT.

9. Click **Open**.

Note:

If you have not connected to this particular server before, SSH prompts you to accept the server's 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 you connect through the interface on the Services laptop computer, if you save the host key, the host is identified as 192.11.13.6. If you later connect to a different server through the laptop interface, this new host also shows as 192.11.13.6, but it has a different key. You get a prompt in this case because it appears that the host key has changed.

10. If necessary, click **Yes** to accept the server's host key.

The system displays the PuTTY window.

11. Log in as **craft**.

Connecting to the server directly

To access the server directly, use a computer with the following minimum specifications:

- ┆ A Windows 2000 or Windows XP operating system
 - ┆ 32-MB of RAM
 - ┆ 40-MB of available disk space
 - ┆ An RS-232 port connector
 - ┆ A network interface card (NIC) with a 10/100BaseT Ethernet interface
 - ┆ A 10/100 BaseT Ethernet, category 5 or better, cross-over cable with an RJ45 connector on each end (MDI to MDI-X)
 - ┆ A CD-ROM drive
1. Plug one end of the CAT5 cable into the Services access port on the back of the server. For more information, see [Figure 16: Services laptop computer connected directly to the S8730 Server](#) on page 98 or [Figure 17: Services laptop computer connected directly to the S8710 or S8720 Server](#) on page 99.
 2. Plug the other end of the CAT5 cross-over cable into the NIC on your computer. Use a NIC adapter if necessary.
 3. Configure your network connection
 - ┆ IP address: 192.11.13.5
 - ┆ Subnetwork mask: 255.255.255.252

For specific information, see [Configuring the network for Windows 2000 and XP](#) on page 104.

Once you connect, use a terminal emulation program or a Web browser to administer the server.

Figure 16: Services laptop computer connected directly to the S8730 Server

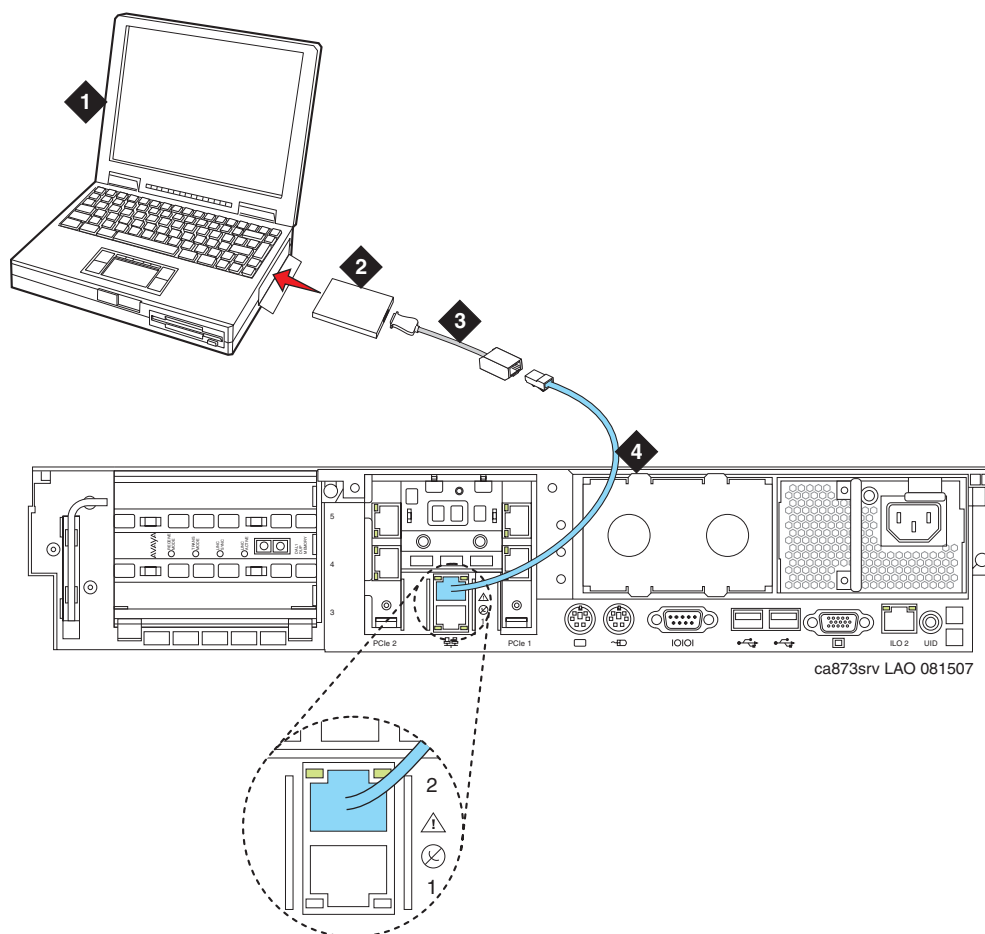


Figure notes:

- | | |
|---------------------------------|-------------------------------------|
| 1. Services laptop computer | 3. NIC adapter cable (if necessary) |
| 2. Network interface card (NIC) | 4. CAT5 cross-over cable |

Figure 17: Services laptop computer connected directly to the S8710 or S8720 Server

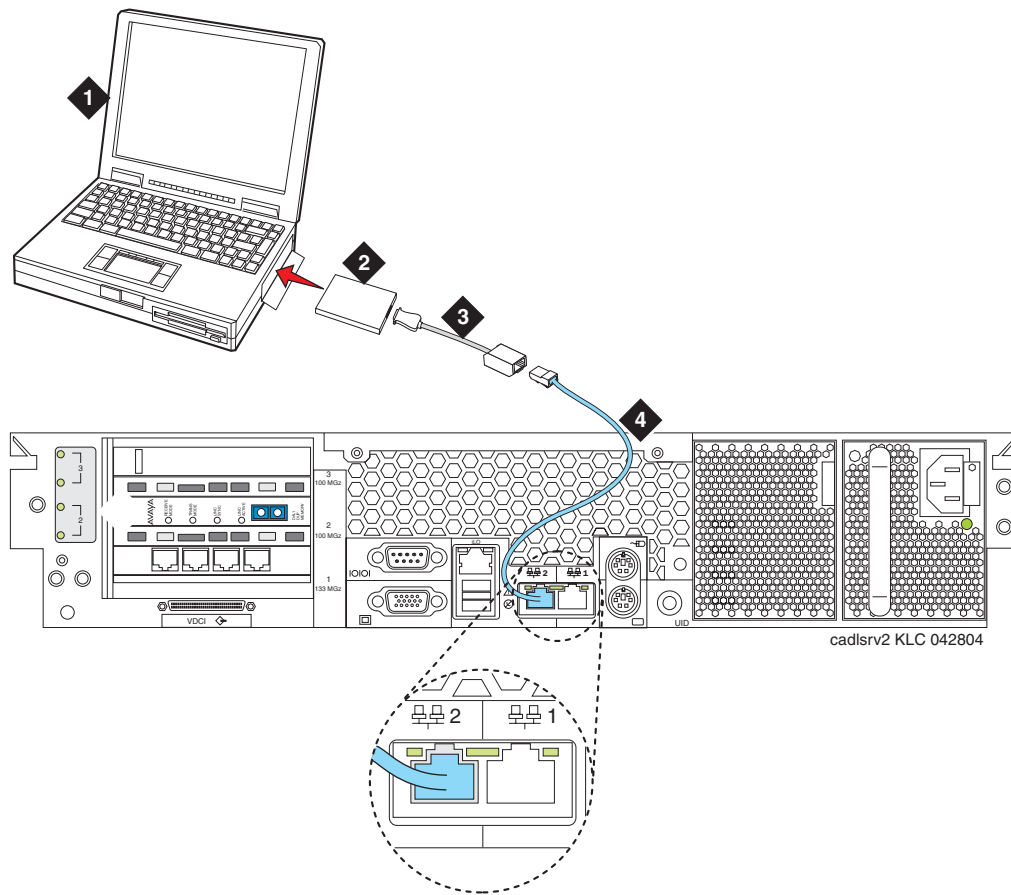


Figure notes:

- | | |
|---------------------------------|-------------------------------------|
| 1. Services laptop computer | 3. NIC adapter cable (if necessary) |
| 2. Network interface card (NIC) | 4. CAT5 cross-over cable |

Connecting to the server remotely over the network

You can use any computer to connect to the server through a LAN. The security settings on the LAN must allow remote access.

1. Open a Web browser or a terminal emulation application.
2. In the address field, enter the IP address or the DNS host name that is assigned to the server that you want to access.

Enter the address of the *active (alias)* server to connect to the active server.

Connecting to the server remotely over a modem

Note:

Remote access over a modem is for Avaya services support access only and not for routine administration. Because the server uses the same modem line to report alarms, the server cannot report new alarms while the line is in use.

You can access the server through an analog modem. The remote connection requires a minimum data speed of 33.5 kilobits per second.

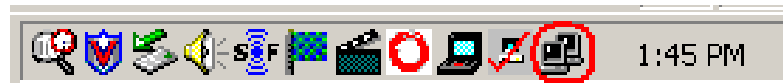
1. Launch the dial-up connection program, which varies depending on your operating system. Generally, you can access the program through the My Computer or the Control Panel folders. For more information, see the Help system of your computer.
2. To open the New Connection wizard, double-click **Make New Connection**.
3. Within the wizard, depending on your operating system, you may be asked to:
 1. Assign a name to the connection.
 1. Select dial-up to the network for the network connection type.
 1. Select the modem you will be using for the dial-up connection.
 1. Enter the appropriate telephone number to access the active server. For the customer-supplied telephone numbers, see the completed *Electronic Preinstallation Worksheet*.
 1. Under Advanced, select **PPP** and log on manually. You might have to type a user name and password, depending on whether or not the server that you are dialing into has a non-null CHAP secret key. If you need a user name and a password, use **craft** for the user name and ignore the password field.
4. Click the connection name or icon, if created. Wait for connection.
5. When prompted, enter your remote access login name and password.

6. When the system displays the `Start PPP now` message, click **Done**. When you see the Connection Complete dialog box, your computer is connected to the server.
7. Open an SSH session using PuTTY or other client.
See [Accessing the command line interface of the server with SSH](#) on page 95 for more information.
8. Within the SSH client, type the IP address of the active server.

Finding the IP address of the active server

To find the active server IP address on a duplicated system:

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



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

Accessing the System Management Interface

You can administer the server through the System Management Interface. Access the System Management Interface when connected:

1. Over the customer network with MS Internet Explorer 6.0 or 7.0.
1. Directly to the Services port on the server. For more information, see [Figure 16: Services laptop computer connected directly to the S8730 Server](#) on page 98 or [Figure 17: Services laptop computer connected directly to the S8710 or S8720 Server](#) on page 99.

To access the System Management Interface, you must first bypass any proxy servers.

1. In Internet Explorer, click **Tools > Internet Options**.
2. Click the **Connection** tab.
3. Click **LAN Settings** in the lower right, then click **Advanced**.
4. In the Exceptions box after the last entry, type **192.11.13.6**
5. Click **OK** to close each of the dialog boxes.

Appendix A: Server access

6. Open the MS Internet Explorer Web browser to access the System Management Interface.
 - 1 If you are connected directly, in the **Address** field, type **192.11.13.6**.
 - 1 If you are connected remotely through a modem, in the **Address** field, type in the IP address or the DNS host name of the server.

Note:

The first time that you log in, you see a message that asks you to install a security certificate. Follow the instructions for your particular browser to accept the certificate. You can also install the certificate on your computer with the instructions in the online Help for your browser.

7. When prompted, log in.
8. When the system displays a message `Do you want to suppress alarms?`, select **Yes**.
9. From the Administration menu, click **Server (Maintenance)**.

Accessing the SAT

Use a remote Secure Shell (SSH) or terminal emulation session to access the Communication Manager SAT command line prompt.

Type of connection	Procedure
Using SAT with SSH:	See Accessing the command line interface of the server with SSH on page 95.
Using SAT with Terminal Emulation	<p>To use a command line interface in a terminal emulation window, open your terminal emulation application. Configure the terminal emulation program port settings as follows:</p> <ul style="list-style-type: none"> ┆ Speed: 115200 baud or 9600 baud if you use a serial modem connection ┆ No parity ┆ 8 data bits ┆ 1 stop bit ┆ No flow control <p>NOTE: Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are the only terminal emulation programs that Avaya supports.</p> <p>Use either the IP address or the DNS host name to establish a network connection to the <i>active</i> server. Use port 5023 for this connection. Use SAT commands on the active server only. When prompted, log in to the server as craft.</p>

Logins for Avaya technicians and Business Partners

Avaya field technicians and Business Partners must use a Services login such as **craft** or **dadmin** to perform initial configuration and upgrades. An Avaya field technician can use a unique password that is assigned to the customer system.

After the Avaya authentication file is installed, Communication Manager has a password for the craft login that is unique to the customer system and available when you are connected directly to the server. If the system is configured without ASG, then all security authentications are through passwords. If ASG is turned on, then all authentication is through ASG except for logins over the service port which require a password. The revised password is recorded by RFA and is obtained from ASG Conversant at 1-800-248-1234 or 1-720-444-5557.

Customers can set up their own logins to access Avaya servers. You must have superuser permission to create or change logins and passwords. NOTE: do not start login IDs with a number. For more information, see the *Avaya Communication Manager Basic Administration Quick Reference* (03-300363).

Configuring the network for Windows 2000 and XP



Important:

Write down the original settings for use in case you need to revert to the original configuration.

1. On your computer that is connected to the services port, right-click **My Network Places** and left-click **Properties** to display the Network Connections window.

Windows 2000 or Windows XP should automatically detect the Ethernet card in your system and create a LAN connection. More than one connection might appear.
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**.
6. Make a note of any IP addresses or other entries that you have to clear. You might need to restore them later to connect to another network

Enter the following:

- ┆ IP address: 192.11.13.5
 - ┆ Subnet mask: 255.255.255.252
7. Select **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
 8. Click **Advanced** at the bottom of the dialog box to display the Advanced TCP/IP Settings dialog box.
 9. Click the **DNS** tab. Ensure no DNS server is administered. The address field should be blank.
 10. Click **OK** and **Close** to close all the windows.

Setting the browser options for Internet Explorer 6.0

A connection session to a server might time out when connected through a proxy server. To avoid having the server time out during a session, add the server host names or IP addresses to the list of host names and IP addresses.

To set browser options for Internet Explorer 6.0:

1. In Internet Explorer 6.0, click **Tools > Internet Options**.
2. Select the **Connection** tab.
3. Click **LAN settings**, then click **Advanced**.
4. In the **Do not use proxy server for addresses beginning with** field, type the IP address for each server you intend to access remotely.

If the IP addresses have the first or first and second octets the same, you can shorten the addresses to xxx.xxx.* (example, 135.9.*).

5. Click **OK** to close each dialog box.

Appendix B: Installation troubleshooting

This section provides some simple strategies to help you troubleshoot an installation of a server. This section includes:

- | [Troubleshooting the installation of the server hardware](#) on page 107
- | [Troubleshooting the configuration of the server hardware](#) on page 108
- | [Troubleshooting the installation of the license file and the Avaya authentication file](#) on page 110

Troubleshooting the installation of the server hardware

Problem	Possible solution
No power to the UPS	<ul style="list-style-type: none"> Ensure that the UPS is plugged into the outlet. Ensure that the outlet has power. For other solutions, see the user guide for the UPS.
No power to the Ethernet switch	<ul style="list-style-type: none"> Ensure that the Ethernet switch is plugged into the UPS or the outlet. Ensure that the UPS or outlet has power. For other solutions, see the user guide for the Ethernet switch.
No power to the server	<ul style="list-style-type: none"> Ensure that the server is plugged into the UPS. Ensure that the UPS has power. Push the power button on the front of the server.
The servers are not shadowing	<ul style="list-style-type: none"> Make sure you are using a cross-over cable. Make sure fiber optic cable is plugged in correctly, RX to TX and TX to RX.
The IPSI LEDs flash	<ul style="list-style-type: none"> Ensure that the IPSI is in the correct slot. Use slot 1 for the G650 Media Gateway. Ping the IPSI from server. Ping the server from the IPSI.

Troubleshooting the configuration of the server hardware

Troubleshooting the configuration of the server hardware

Problem	Possible solution
Cannot log in to the UPS subagent	<ul style="list-style-type: none"> 1 Ensure that the SNMP subagent is installed in the UPS. 1 Ensure that you are connected to the correct Ethernet port. 1 Ensure that you have the correct login ID and password. For more information, see the user guide for the SNMP subagent. 1 Ensure that the network card on the laptop computer is configured correctly.
Cannot log in to the Ethernet switch	<ul style="list-style-type: none"> 1 Ensure that you are connected to the correct Ethernet port. (On the Ethernet switch, the correct port is labeled Console) 1 Ensure that you have the correct login ID and password. See the user guide for the Ethernet switch. 1 Ensure that the network card on the Services laptop computer is configured correctly.
Cannot log in to the server	<ul style="list-style-type: none"> 1 Check the link LED on the server. If the LED is off, a cable or hardware problem exists. 1 Ensure that you are using SSH and not telnet. 1 Ensure that you are connected to the Services Ethernet port. 1 Ensure that you are using a cross-over cable between the Services laptop computer and the server. 1 Ensure that the ARP cache is cleared on the Services laptop computer. In an MS-DOS window, type arp -d 192.11.13.6 and press Enter. 1 Ensure that you have connectivity. In an MS-DOS window, type ping 192.11.13.6 and press Enter. 1 Ensure that the NIC on the Services laptop computer is configured correctly.
Cannot access the Avaya Installation Wizard	<ul style="list-style-type: none"> 1 Ensure that you are plugged into the Services port. 1 Ensure that you are using SSH and not telnet. 1 Ensure that you are using the correct IP address, 192.11.13.6 1 Ensure that you are using the correct login and password. 1 Ensure that the NIC on the laptop is configured correctly.
1 of 2	

Troubleshooting the configuration of the server hardware (continued)

Problem	Possible solution
Cannot use SAT commands	<ul style="list-style-type: none"> 1 Ensure that you are using the correct IP address, 192.11.13.6 and port 5023. 1 Ensure that you are using SSH and not telnet. 1 Ensure that you are using the correct login and password. 1 Make sure you are logged onto the active server.
Cannot ping out to the customer network	<ul style="list-style-type: none"> 1 Ensure that in the LAN security settings “output from server” for icmp is enabled.
Cannot ping the server from the customer network	<ul style="list-style-type: none"> 1 Ensure that in the LAN security settings “input to server” for icmp is enabled.
Cannot access the server remotely	<ul style="list-style-type: none"> 1 Ensure that in the LAN security settings “input to server” is checked for SSH (Linux commands), https (Web access), and def-sat (SAT commands access). Change the LAN security settings on the Web interface with a direct connection to the server.
The LED display on IPSI is flashing	<ul style="list-style-type: none"> 1 The IPSI LED is not programmed with the switch and the location (DHCP) 1 An IP address is not assigned to the IPSI LED (static IP addressing).
Cannot access the IPSI for static addressing	<ul style="list-style-type: none"> 1 Ensure that you are plugged into the Services (top) port on the IPSI. 1 Ensure that the ARP cache is cleared on the Services laptop computer. In an MS-DOS command window, type arp -d 192.11.13.6 and press Enter.
No “V” shows on the IPSI LED	<ul style="list-style-type: none"> 1 The IPSI is not connected to the Ethernet switch or the network. Connect a cable to the bottom port on the faceplate and to the Ethernet switch or the customer network. 1 Make sure port on the Ethernet switch that is assigned to that IPSI is enabled.
The “V” on the IPSI LED is not filled in	<ul style="list-style-type: none"> 1 An IP address is not assigned to the IPSI. 1 The IPSI is not administered.
The system generates an alarm when first connect to IPSI	<ul style="list-style-type: none"> 1 The IPSI does not have the current firmware. Upgrade the firmware.
2 of 2	

Troubleshooting the installation of the license file and the Avaya authentication file

Problem	Possible solution
Cannot get files from the RFA site	<ul style="list-style-type: none"> 1 Provide the correct SAP number. 1 Provide the serial number for the reference IPSI.
Cannot install the license file	<ul style="list-style-type: none"> 1 Ensure that two license files do not exist on the server. If so, delete one of the files. 1 The file might be corrupt. Download the file again from the RFA site. 1 Use binary mode to upload the file.
The server is in no-license mode	<ul style="list-style-type: none"> 1 The license file does not have an IP address yet. This situation is normal when the license file is first installed because the file cannot see the IPSI. 1 After 30 minutes, the license file has not located the reference IPSI. In a SAT session, type reset system 1 and press Enter to reset the 30-minute clock.
Cannot use the administration commands	<ul style="list-style-type: none"> 1 The server might be in no license mode because the 30-minute timer lapsed. In a SAT session, type reset system 1 and press Enter to reset the 30-minute clock.
ASG does not work	<ul style="list-style-type: none"> 1 Re-install the Avaya authentication files.
Cannot install the authentication file	<ul style="list-style-type: none"> 1 Administer a super-user login on the active server.

Index

Numerical

8730 Server configurations [17](#)

A

access server
 directly [97](#)
 remotely over modem [100](#)
 remotely over network [100](#)
 accessing [101](#)
 accessing System Management Interface [101](#)
 accessing the server [36](#)
 add
 IP interface information [60](#)
 media gateways [58](#)
 administer
 IPSI circuit pack [65](#)
 AIW. See Avaya Installation Wizard
 alarm activation level
 setting [61](#)
 alarms
 enabling to INADS via SNMP [80](#)
 setting selected traps [30](#)
 to INADS by way of modem, enabling [79](#)
 viewing. [77](#)
 ARP cache, clearing [35](#)
 Avaya Installation Wizard, using [42](#), [46](#)

B

backing up files to compact flash [80](#)

C

C363T or C364T Ethernet switch
 configuring [31](#)
 LEDs [89](#)
 security alert [31](#)
 clearing ARP cache [35](#)
 collocated servers, connecting to [23](#)
 command line interface. [103](#)
 Communication Manager
 installing software. [35](#)
 compact flash, backing up to [80](#)
 configure
 Avaya C363T or C364T Ethernet switch [31](#)

media server 2 [53](#)
 modem [48](#)
 network interface card (NIC) [52](#)
 server [39](#), [57](#)
 UPS [27](#)
 connect to customer network [17](#)
 connection to LAN, verifying. [47](#)
 customer network, connecting to [17](#)

D

date and time, verifying [76](#)
 daylight savings rules
 location [75](#)
 setting [74](#)
 DHCP IP addressing
 IPSI circuit pack [65](#)
 using [70](#)
 diffserv parameters, setting [68](#)
 direct access to server [97](#)
 disable unused Ethernet switch ports [77](#)
 disconnecting from server. [53](#)
 duplicated IPSIs, enabling. [61](#)

E

enable Ethernet switch ports [77](#)
 ESS compatibility. [50](#)
 Ethernet interface assignments [44](#)
 Ethernet switch
 configuring [33](#)
 default IP addresses. [31](#)
 disabling unused ports. [77](#)
 preparing to configure [32](#)
 Extra Large configuration [50](#)

F

faceplate
 TN2312BP circuit pack [91](#)
 firewall settings. [51](#)

I

INADS
 enabling alarms to by way of modem [79](#)
 inputting translations [57](#)
 installation

Index

troubleshooting	107
using the Wizard	42, 46
installing	
Communication Manager software	37
translation file	61
interchanging servers	54
IP address	
finding for the active server	101
set static	66
use DHCP	70
IP address, set static.	66
IP interface	
enabling control	63
upgrading firmware version	62
verify translations	62
IP interface information	
adding to translations	60
IPSI	
connecting to	65
enabling duplication.	61
LEDs	91
program switch ID and cabinet.	65

L	
LED	
additional information	88
LEDs	
Avaya Ethernet switches	89
IPSI	91
S8700-series Server	86
S8730 Server.	84
UPS	90
license file, testing	83
license, verifying status.	63
location	
setting for media gateways	75
login, super-user.	40
LSP compatibility	50

M	
manual configuration	
configuration, manual method	42
media gateways, adding	58
media server	
applying power	36
media server 2	
configuring	53
modem	
access to server	100
configuring	48
connect to server	23
modem options, setting.	24
modem, enabling alarms to INADS	79

N

network interface card (NIC)	
configuring	52
network time server (NTP), enabling	51

P

PNC license settings for S8700	13
post installation tasks	81
power	
applying to media server	36
pre-installation tasks at the installation site	13
Processor Ethernet	24

R

RAID level 1 (S8730 server).	17
remote access to server	
over modem	100
over network	100

S

S8700	
active server, finding the IP address	101
port connections.	18
S8700-series Media Server	
PNC license settings	13
S8700-series Server	
LEDs	86
S8730 Server	
LEDs	84
saving translations	57, 61
separated servers, connecting to	
server	
accessing.	36
configuring	39, 57
disconnecting from	53
LED, additional information	88
LEDs	84, 86
verify connectivity	62
verifying LAN connection.	47
server configuration, manual method.	42
set	
alarm activation level	61
daylight savings rules	74
selected traps (alarming).	30
static IP address	66
set static IP address	66
SNMP	
preparing to configure	29
SNMP modules	
administering	30

software, installing Communication Manager	37
spanning tree	
enabling	33
setting version	33
SSH	
about	25
static IP addressing	
IPSI circuit pack	65
setting	66
static IP addressing, setting.	66
super-user login	40

T

Telnet	
configuring for Win2000/XP	36
terminal emulation	103
testing	
license file	83
server installation	83
TN2312BP	83
TN2312BP	
faceplate	91
LEDs	91
program switch ID and cabinet.	65
TN2312BP, testing.	83
translation file	
installing	61
translations	
inputting	57
IP interface.	57
saving	57 , 61
verifying	73
troubleshooting, server installation	107

U

upgrading	
IP interface firmware version	62
UPS	
default IP addresses for S8700	28
LEDs	90
security alert	27
SNMP module	27
UPS, configuring.	27
using DHCP IP address	70
using this documentation	12

V

verify	
connectivity to servers	62
date and time.	76
IP interface translated.	62

license status	63
server connection to LAN	47
translations	73
view alarms	77
VLAN parameters, setting.	68

W

Wizard, installation	42 , 46
--------------------------------	---

