Installing and Configuring the Avaya S8500-Series Server

Release 5.2

03-300143
Release 5.2
May 2009
Issue 7

© 2010 Avaya Inc.
All Rights Reserved.

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.

Copyright 2010, Avaya Inc.
All Rights Reserved

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 IECEE 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 quarantee 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 reveiver.
- Connect the equipment into an outlet on a circuit different from that to which the reveiver 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 materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

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

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

European Union Battery Directive



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

Japan

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

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

Downloading documents

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

http://www.avaya.com/support

Contents

Chapter 1: Introduction 13
Audience 13
How to use Avaya installation documents 14
Preinstallation tasks to complete at the customer site 15
Verifying that all the required equipment is on site 15
Ensuring that the preinstallation tasks are complete 15
S8500 hardware 16
Equipment specifications 18
About the Server Availability Management Processor 22
About SAMP functionality 22
About SAMP connections 22
About SAMP software 24
About server port connections 25
S8500 port connections 25
About modem connections 27
Modem options 28
About media gateways 28
About Processor Ethernet 28
About S8500 LSP mode 30
S8500 LSP license file 31
About SSH 31

Chapter 2: SNMP configuration 33
Configuring the SNMP modules in the UPS 33
Default IP addresses for the UPS 34
Prerequisites for configuring the SNMP module 34
Administering the SNMP module 35
Setting selected traps (alarming) 36
Configuring the SNMP subagent in the Avaya Ethernet switch (if used) 36
Default IP addresses for the Ethernet switch 37
Preparing to configure the Ethernet switch 37
Configuring the Ethernet switch 38

Chapter 3: Communication Manager installation 41
Clearing the ARP cache on the laptop 41
Applying power to the server 42
Accessing the server 42
Configuring Telnet for Windows 2000 and Windows XP 42

Installing Communication Manager 43

Chapter 4: Server configuration 45
Methods of Configuring a server 45
Opening the System Management Interface 46
Creating a super-user login 46
Copying license and authentication files to the server 47
Installing the license and authentication files 47
Installing the license file. 47
Installing the authentication file 48
Configuring the server manually 48
Setting the date, time, and time zone. 48
Rebooting the server 49
System Management Interface configuration screens 49
Ethernet interface assignments. 51
Performing the manual configuration 51
Avaya Installation Wizard 52
About the Avaya Installation Wizard 52
Running the Avaya Installation Wizard. 53
Verifying the RMB IP information. 53
Upgrading the SAMP firmware 54
Verifying the server connection to the customer LAN (if provided) 54
Configuring the modem 55
Enabling firewall settings 55
Enabling network time servers 56
Checking LED activity on the dual NIC. 58
Configuring the NIC 58
Release the server 60

Chapter 5: IP interface configuration 61
Connecting to the IPSIs 61
IPSI address configuration 61
Programming the IPSI for static addressing 62
Setting the VLAN and diffserv parameters 65
Programming the IPSI for DHCP addressing 66

Chapter 6: IP interface translations 69
Inputting initial system translations 69

Adding media gateways 70
Enabling the IPSI. 71
Adding the IPSI to the system 72
Setting the alarm activation level 72
Saving translations 73
Verifying connectivity to the server 73
Verifying that the IPSIs are translated 73
Upgrading the IPSI firmware version (if necessary) 73
Enabling control of the IPSIs 74
Verifying the license status 74

Chapter 7: S8500 Server Roles 75
Configuring an S8500 server as a main server 75
Installing and configuring an S8500 Server as an LSP 76
Configuring the server as an LSP 77
Administering the primary controller 78
Enabling license server capability on a media gateway 79
Installing and verifying the license on the new LSP 79
Opening the TCP ports on the S8500 LSP 80
Resetting the S8500 LSP 81
Verifying that the primary controller identifies the new LSP 81
Readministering media gateways to point to the LSP 81

Chapter 7: Postinstallation administration 83
Verifying translations 83
Setting rules for daylight savings time 84
Setting locations (if necessary) 85
Verifying the date and the time (main server only) 86
Clearing and resolving alarms 87
Enabling and disabling the Ethernet switch ports 87
Enabling alarms to INADS by way of a modem 89
Enabling alarms to INADS by way of the SNMP module 90
Backing up files to the compact flash media 90
Before leaving the site 91

Chapter 8: Installation verification 93
Testing the IPSI circuit pack 93
Testing the license file 93
S8500 LEDs 94
Additional server LED information 97
Avaya C360 Ethernet switch LEDs 98
UPS LEDs 99
TN2312BP IPSI LEDs 100

Chapter 9: Installing the Avaya S8510 Server Family and its Components 105
Overview of server and components 105
Server components 105
Specifications 106
Environmental specifications 107
Front view of server 107
Back view of server 108
Dual Network Interface Card (NIC) 109
SAMP overview 109
Modem 110
Compact flash reader 110
Related hardware 111
LEDs 111
Front panel LEDs 111
Back panel LEDs 112
LED conditions and patterns 112
Dual NIC LEDs 114
Server rack installation 114
Customer-provided equipment 114
Avaya-provided equipment 115
Recommended tools and supplies 115
Safety instructions 115
Installation checklist 117
Marking the rack 118
Prerequisites 118
Attaching rails to the server 120
Attaching the rails to the rack 121
Installing the server in the rack 121
Prerequisites 121
Next steps 122

Powering up the server 122
Next steps 123
Adding a second power supply 123
Next steps 123
Troubleshooting the hardware installation 123
Avaya customer equipment is missing. 123
The server has no power 124
LCD Status messages 124
LCD status message explanations 124
Removing LCD status messages 131

Chapter 10: Configuring Communication Manager on the S8510 Server 133
S8510 port connections 133
S8510 BIOS Upgrade Feature 134

Appendix A: Server access 135
Accessing the command line interface of the server with SSH 135
Connecting to the server directly 137
Connecting to the server remotely over the network 140
Connecting to the server remotely over a modem 140
Accessing the System Management Interface 141
Accessing the SAT. 142
Logins for Avaya technicians and Business Partners 142
Configuring the network for Windows 2000 and XP 143
Setting the browser options for Internet Explorer 6.0 144

Appendix B: Installation troubleshooting 145
Troubleshooting the installation of the server hardware 145
Troubleshooting the configuration of the server hardware 146
Troubleshooting the installation of the license file and the Avaya authentication file 148

Index 149

Chapter 1: Introduction

Use these procedures to install Communication Manager and configure a new Avaya S8500 Server and the associated components in an IP-connected port network (IP-PNC) configuration.

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

- The System Management Interface.
- 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:

- Preinstallation tasks to complete at the customer site on page 15
- Configuring the SNMP modules in the UPS on page 33
- Server configuration on page 45
- IP interface translations on page 69
- IP interface configuration on page 61
- Postinstallation administration on page 83
- Installation verification on page 93
- Installing the Avaya S8510 Server Family and its Components on page 105
- Configuring Communication Manager on the S8510 Server on page 133
- Server access on page 135
- Installation troubleshooting on page 145

Audience

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

- Trained field installation and maintenance personnel
- Technical support personnel
- 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:

- In this document, see:
  - Preinstallation tasks to complete at the customer site on page 15. This section describes the tasks that you must complete before you start the installation.
  - Equipment specifications on page 18 for the technical specifications for the hardware.
- For how to install and connect the hardware, see *Quick Start for Hardware Installation: Avaya S8500 Server* (555-245-701).
- For how to install an updated version of the Avaya Server Availability Management Processor (SAMP) and configure the SAMP, see *Using the Avaya Server Availability Management Processor* (03-300322).
- 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 33
  - Server configuration on page 45
  - IP interface translations on page 69

Important:
If the S8500 Server is configured as an LSP, skip the following section.

- 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 61 to program the IP interface.
  - Postinstallation administration on page 83
  - Installation verification on page 93
  - Server access on page 135
  - Installation troubleshooting on page 145 if problems occur during the installation.

Preinstallation tasks to complete at the customer site

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

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.

- 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.
- Verify that the rail kit to support the server is available to install (S8400 installed in a G650 carrier only).
- Verify that the rail kit to support the server is available to install.

- 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.
- Verify that the equipment racks are grounded per local code. See *Job Aid: Approved Grounds* (555-245-772).
- Verify that the customer-provided AC power to the rack is from a nonswitched outlet.
- Verify that cables for theTN2312BP (IPSI) circuit packs are labeled and run from the control hardware rack to the port networks or that appropriate connectivity is provided.

S8500 hardware

The hardware components for the S8500C and 8500B versions of the S8500 Server are very similar but the layout of the components on the front and back panels are different. The following four diagrams show the hardware components on the front and back panels of the S8500C and S8500B with the default port assignments.

Figure 1: S8500C front panel

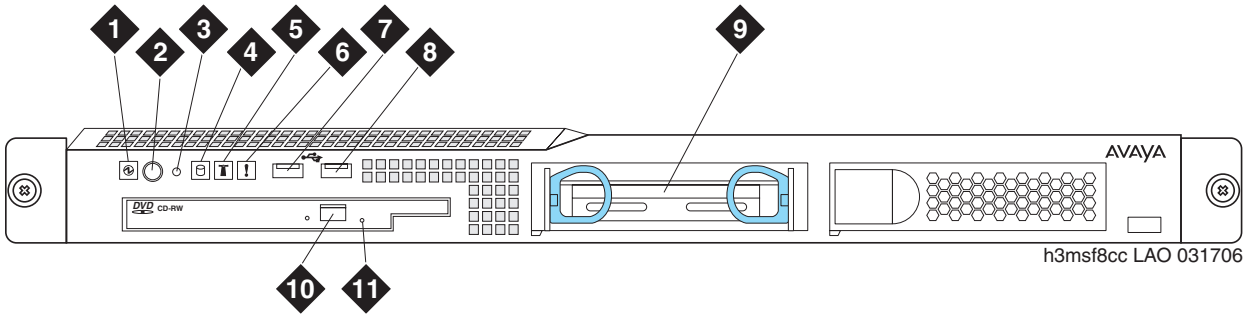
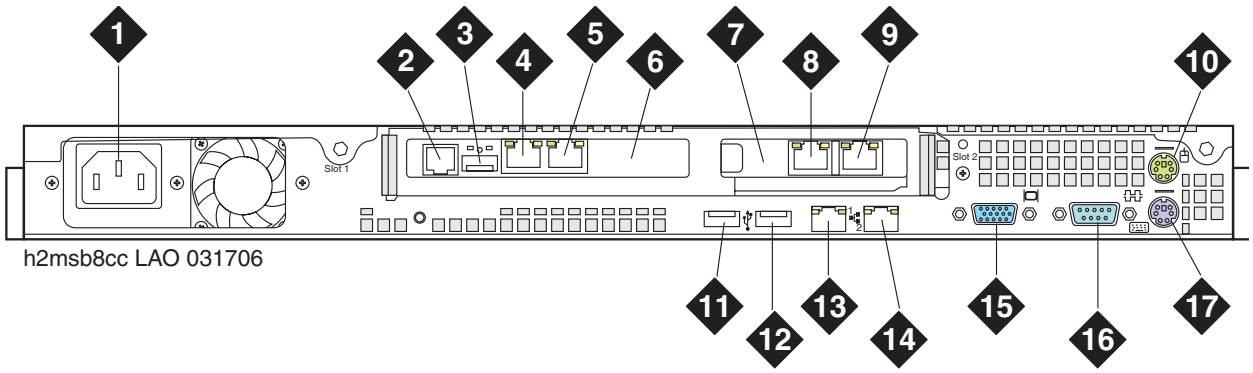


Figure notes:

1. Power-on LED
2. Power button
3. Reset button
4. Hard disk drive activity LED
5. Locator LED
6. System error LED
7. USB port
8. USB port
9. Hard disk drive
10. CD eject button
11. CD-ROM drive activity LED

Figure 2: S8500C back panel

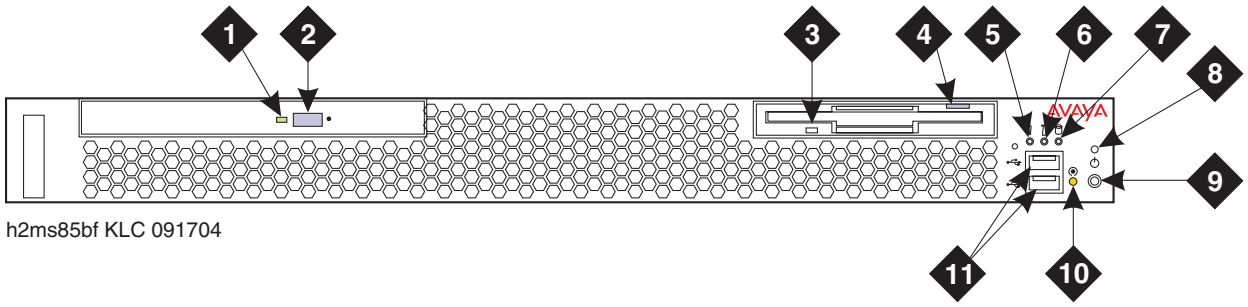


h2msb8cc LAO 031706

Figure notes:

1. Power cord connector
2. SAMP power
3. USB connection to USB modem
4. Ethernet port (SAMP Eth 1)
5. SAMP Services port (SAMP Eth 2)
6. SAMP card
7. Dual NIC
8. Ethernet 4
9. Ethernet 3
10. Mouse connector
11. USB port
12. USB port
13. Ethernet 0
14. Ethernet 1
15. Video connector
16. Serial connector
17. Keyboard connector

Figure 3: S8500B front panel



h2ms85bf KLC 091704

Figure notes:

1. CD-ROM drive activity LED
2. CD-ROM eject button
3. Diskette drive activity LED
4. Diskette eject button
5. System error LED
6. System locator LED.
7. Hard disk drive activity LED
8. Power on LED
9. Power control button
10. Reset button — Press to reset the server and run the power-on self-test (POST).
11. USB connections for the compact flash drive.

Figure 4: S8500B back panel

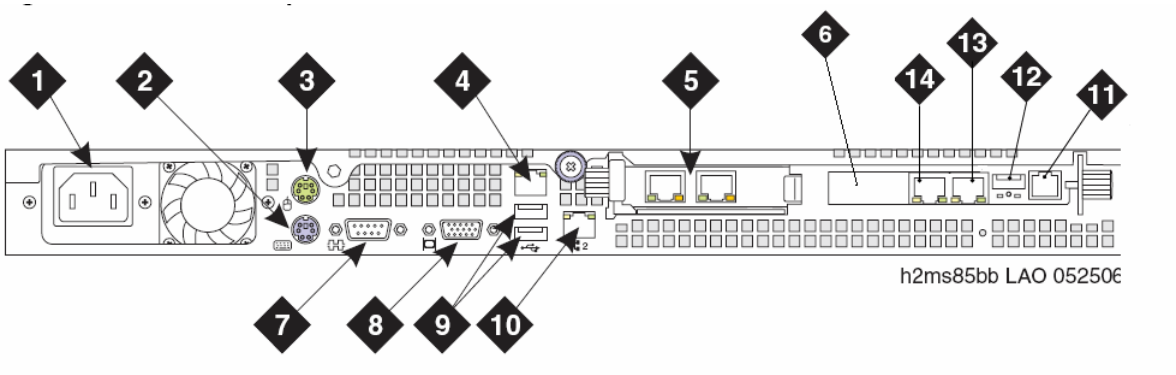


Figure notes:

1. Power cord connector
2. Keyboard connector
3. Mouse connector
4. Ethernet port (Eth 0)
5. Dual NIC with Ethernet ports Eth 2 and Eth 3
6. SAMP card
7. Video connector
8. Serial connector
9. USB ports
10. Ethernet port (Eth 1)
11. SAMP power
12. USB connection to USB modem
13. Ethernet port (SAMP Eth 1)
14. SAMP Services port (SAMP Eth 2)

Equipment specifications

Important:
The TN8400BP cicuit pack is compatible with Communication Manager Release 4.0.3 and later.

The S8500 Server control network components consist of the server, one UPS, and an Avaya-provided Ethernet switch (optional). The physical specifications for the control network components are shown in Table 1.

Table 1: S8500 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: S8500B S8500C	 1.75 x 17 x 20 1.75 x 17 x 22	 4 x 43 x 51 4 x 43 x 56	 1 1	28/13
Ethernet Switch: C363T C364T	 1.75 x 17 x 14.4 1.75 x 17 x 14.4	 4 x 43 x 37 4 x 43 x 37	 1 1	 11/5 11/5
UPS: 700 VA 1500 VA	 3.5 x 17 x 19 3.5 x 17 x 24	 9 x 43 x 48 9 x 43 x 61	 2 2	 34/15 50/23

Table 2 outlines the features and specifications of the Avaya S8500 Server. The differences between the S8500B and S8500C versions are noted.

Table 2: S8500 Server specifications

Feature	S8500B	S8500C
Micro-processors	CPU: 3.0 GHz Pentium (P4) FSB: 800 MHz front-side bus	CPU: 3.2 GHz Pentium (P4) FSB: 800 MHz front-side bus
Memory	One 512 MB PC2100 CL2.5 ECC DDR SDRAM RDIMM	Two 512 MB PC2-4200 CL4 ECC DDR2 SDRAM DIMM
Drives	One 80 GB SATA hard disk drive CD-ROM/DVD-ROM: IDE	One 80 GB SATA hard disk drive CD-ROM/DVD-ROM: IDE
Dual NIC	Optional	One dual NIC card
Slots	Two PCI-X slots - 64 bit/66 MHz Accommodates the SAMP and dual NIC	Two PCI-X slots - 64 bit/66 MHz Accommodates the SAMP and dual NIC

Table 2: S8500 Server specifications (continued)

Feature	S8500B	S8500C
Power supply	300 W (110 VAC or 220 VAC autosensing)	350 W (110 VAC or 220 VAC autosensing)
Integrated functions	Ethernet ports: two 10/1000/100BaseT Ethernet controllers One serial port (not used) Four USB ports (3 not used) Keyboard port (not used) Mouse port (not used) Dual-channel bus mastering IDE controller	Same as the S8500B.

Environmental specifications for the S8500 Servers are shown in Table 3.

Table 3: S8500 Server environmental specifications

Parameter	S8500B Specifications	S8500C Specifications
Acoustical Noise Emissions	Sound power, idling: 65 decibel maximum Sound power, operating: 65 decibel maximum	Same as S8500B Same as S8500B
Environment: Air Temperature	Server on: 50.0°F to 95.0°F (10°C to 35°C) Altitude: 0 ft to 2999 ft (0 m to 914 m) Server off: -40°F to 140°F (-40° to 60° C) Maximum altitude: 6998 ft (2133 m)	 Same as S8500B Same as S8500B Same as S8500B Same as S8500B
Environment: Humidity	Server on: 8% to 80% Server off: 8% to 80%	Same as S8500B Same as S8500B
Heat Output	Minimum configuration: 297 BTU (87 W) Maximum configuration: 512 BTU (150 W)	Minimum configuration: 341 BTU (100 W) Maximum configuration: 1024 BTU (300 W)
Electrical Input	Receptacle U.S.: NEMA 5-15 A Circuit Breaker: 15 A Sine-wave input (47 Hz to 63 Hz) required Input voltage low range: 100 – 127 VAC Input voltage high range: 200 – 240 VAC Input kilovolt-amperes (approximate): 0.09 – 0.15 kVA Amp draw: 100 to 127 V ~ 4.6 A 200 to 240 V ~ 2.3 A	Same as S8500B Same as S8500B Same as S8500B Same as S8500B Same as S8500B Input kilovolt-amperes (approximate): 0.10 – 0.55 kVA Amp draw: 100 to 127 V ~ 6.0 A 200 to 240 V ~ 3.0A

About the Server Availability Management Processor

The Server Availability Management Processor (SAMP) remote maintenance circuit card is preinstalled in the S8500 Server. The SAMP monitors and reports alerts from the S8500 components to provide remote maintenance and serviceability for the server. The SAMP also provides controls to turn on and turn off the power to the server.

About SAMP functionality

The SAMP circuit card:

- Monitors the server boot process, the CM watch dog, the fans, the voltages, and the temperature.
- Reports media-server-failure alarms and other alarms to INADS by way of a modem.

Note:

Modem contention is resolved on a first-come first-serve basis. For example, Services dials into the SAMP, and the server must send out an alarm through the modem interface. Although the modem is busy, the server continues to try to send the alarm.

- Provides the capability to turn on power and to reset the server remotely.
- Provides a secure dial-in connection to the SAMP and the host.
- Provides access to the SAMP and subsequently access to the host by way of the Services laptop.

The SAMP presents a virtual TTY that the server uses when the server must send out alarms through the modem interface (). The system uses the modem that is connected to the USB port on the SAMP card to report alarms on the:

- Server by the server
- Server by the SAMP, such as server reboots.
- SAMP by the SAMP

About SAMP connections

The SAMP card is installed in PCI-X slot 1 of the Avaya S8500 Server. Slot 1 is a full-height, three-quarters length slot.

The SAMP comes in a half-card PCI form factor and is powered externally. The SAMP supports one USB interface and two 10/100 Ethernet ports that are located on the rear of the server.

- SAMP Ethernet 1 is not used.
- SAMP Ethernet 2 is for local access. This port is for on-site services personnel to access the SAMP with the craft login.
- The USB interface is used to connect a USB modem for remote dial-in access. The server and the SAMP share this modem connection for remote maintenance, administration, and alarming. For remote dial-in, the user first establishes a Point-to-Point Protocol (PPP) session that terminates at the SAMP. The user can then use the craft login to establish an SSH (Secure Shell) or an HTTPS (Secure Web) session to the SAMP or the host.

The SAMP also communicates with the host in-band by way of an on-board industry-standard Ethernet controller on the PCI bus of the host with an internal link to the SAMP.

Figure 5: SAMP connections for S8500C shows the locations of the connections on the SAMP for the S8500C. Figure 6: SAMP connections for S8500B on page 24 shows the locations of the connections on the SAMP for the S8500B.

Figure 5: SAMP connections for S8500C

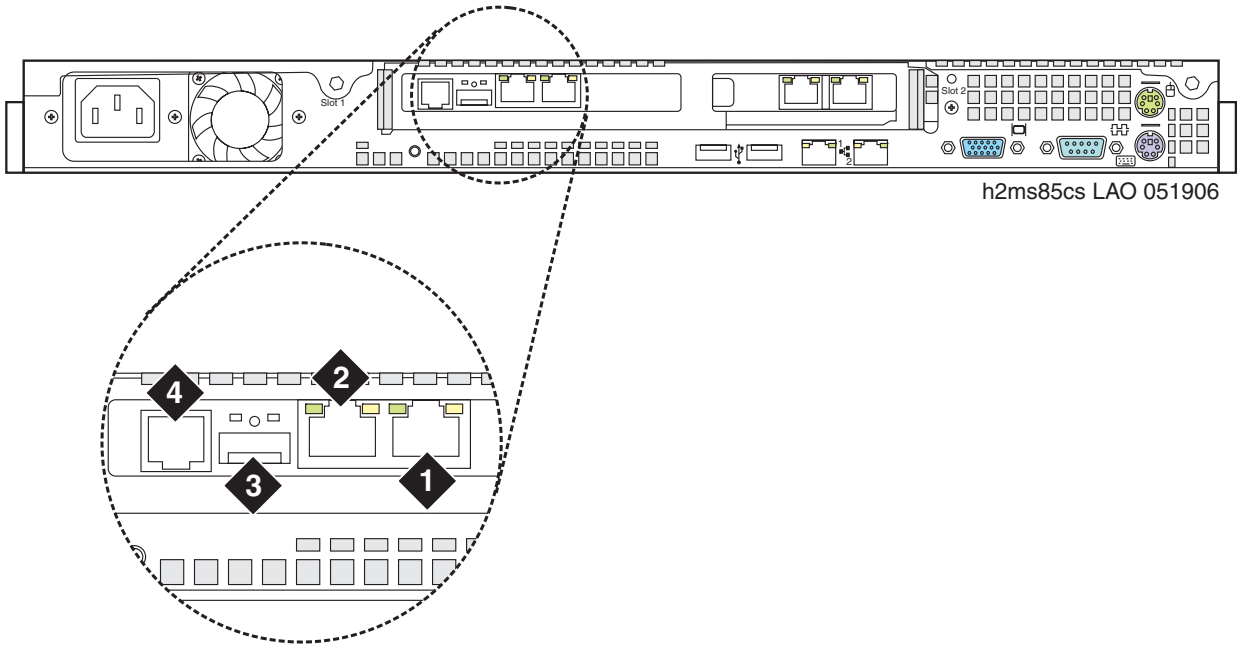
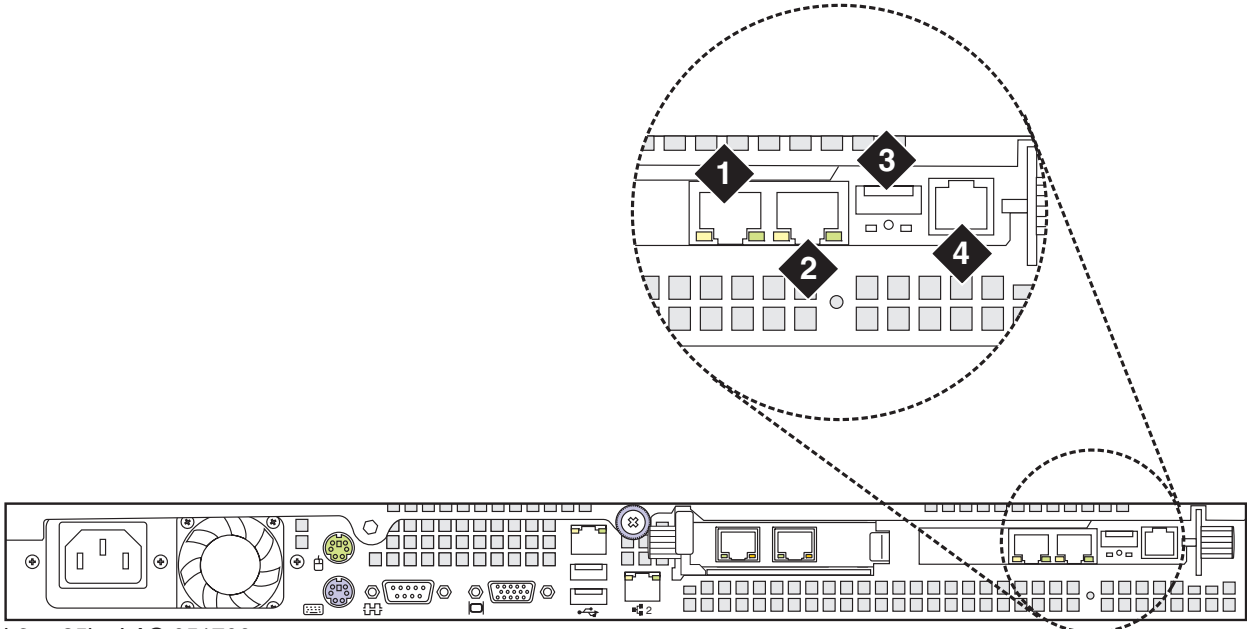


Figure notes:

1. SAMP Eth2—to the services laptop computer (cross-connect CAT5 cable)
2. SAMP Eth1 (not used)
3. USB connection for the modem
4. External power to the SAMP

Figure 6: SAMP connections for S8500B



h2ms85bs LAO 051706

Figure notes:

1. SAMP Eth2—to the services laptop computer (cross-connect CAT5 cable)
2. SAMP Eth1 (not used)
3. USB connection for the modem
4. External power to the SAMP

About SAMP software

The SAMP is shipped from the factory with the software installed and with some default settings. However, you might need to install an updated version of the software, and you must configure the SAMP before you can use it.

If a SAMP software update file is available on the Avaya Support Web site, one of the preinstallation tasks required that you load the file on your laptop: see *Using the Avaya Server Availability Management Processor (SAMP)* (03-300322) for how to install software on the SAMP and change the default settings.

About server port connections

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

S8500 port connections

Use standard CAT5 cables with RJ45 connectors on each end to connect to the various ports. If the S8500 Server has only one port network, connect that port network through the dual NIC. Figure 7: S8500C Server connectivity guide shows typical connectivity for the S8500C Server. Figure 8: S8500B Server connectivity guide on page 26 shows typical connectivity for the S8500B Server.

Figure 7: S8500C Server connectivity guide

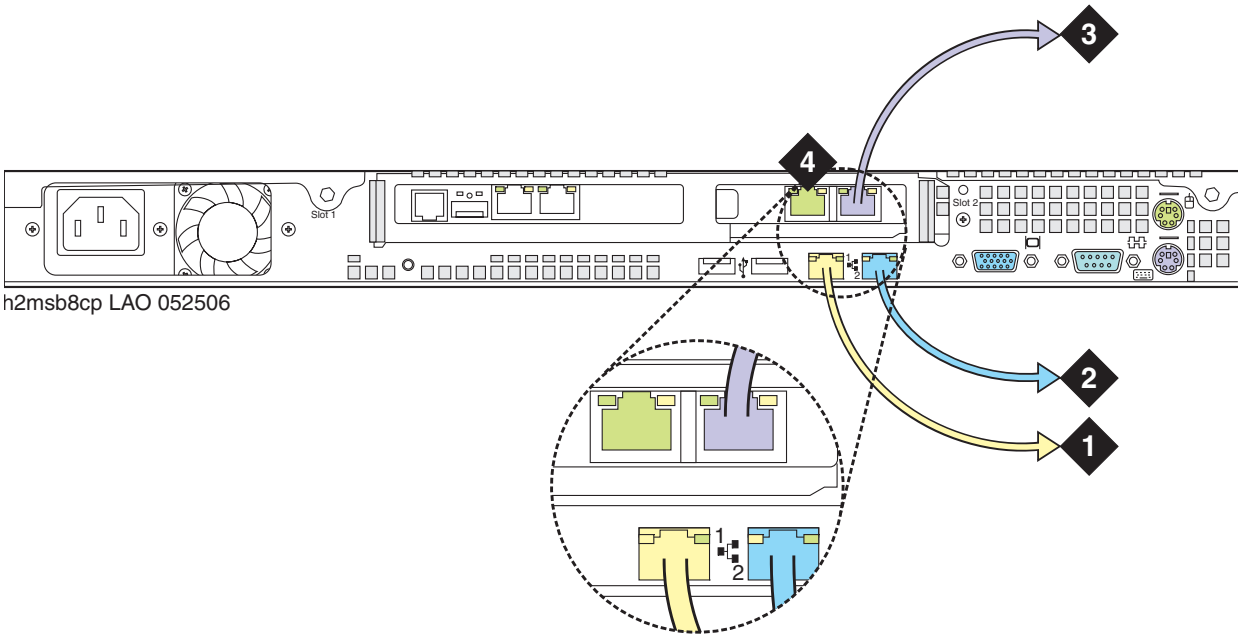


Figure notes:

1. Eth0—To the customer network if the control network is nondedicated. Or, to the control-network Ethernet switch if the control network is dedicated (straight-through CAT5 cable)
2. Eth1—To the Services laptop computer (cross-over CAT5 cable)
3. Eth3—to the customer network if the control network is dedicated (straight-through CAT5 cable)
4. Eth4—Not used

Figure 8: S8500B Server connectivity guide

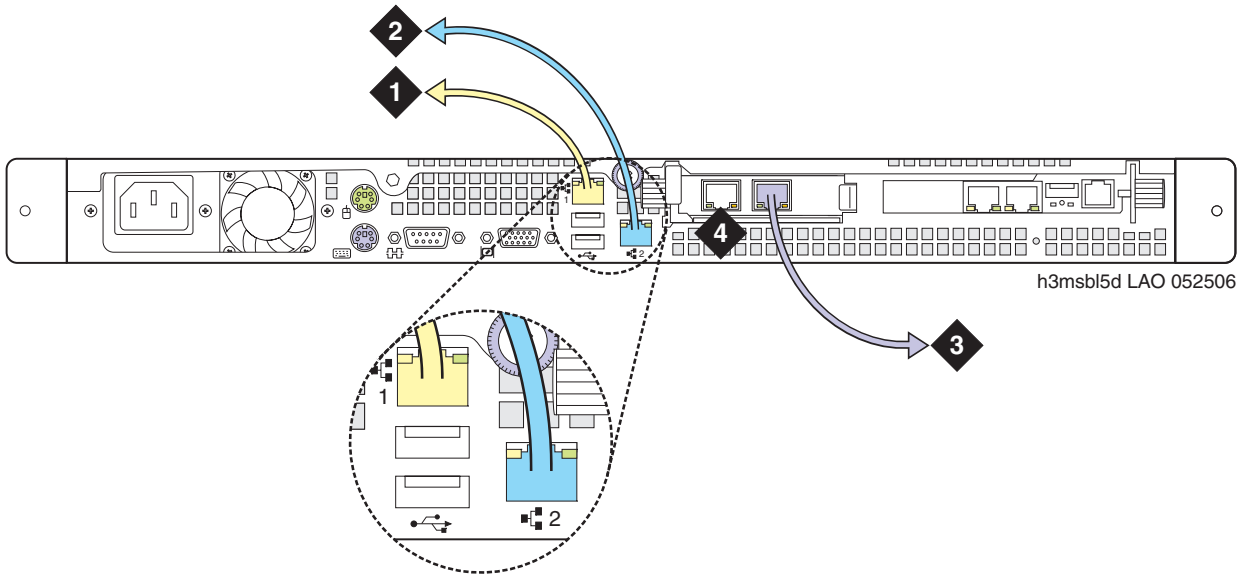


Figure notes:

1. Eth0—To the customer network if the control network is shared. Or, to the control-network Ethernet switch if the control network is dedicated (straight-through CAT5 cable)
2. Eth1—To the Services laptop computer (cross-over CAT5 cable)
3. Eth2—to the customer network if the control network is dedicated (straight-through CAT5 cable)
4. Eth3—Not used

Note:

If the S8500C is configured as an ESS, the port assignments are different:

- Eth0: Control Network A
- Eth3: Control Network B
- Eth4: LAN, if two dedicated control networks are used

In either case, ETH2 is an internal port dedicated to the SAMP.

About modem connections

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

On an Avaya S8500 Server, connect the modem to the USB port on the SAMP.

Avaya defaults on the SAMP set the required options on the SAMP modem. For modem connectivity, see Figure 9: Modem connectivity on the S8500 Server.

Figure 9: Modem connectivity on the S8500 Server

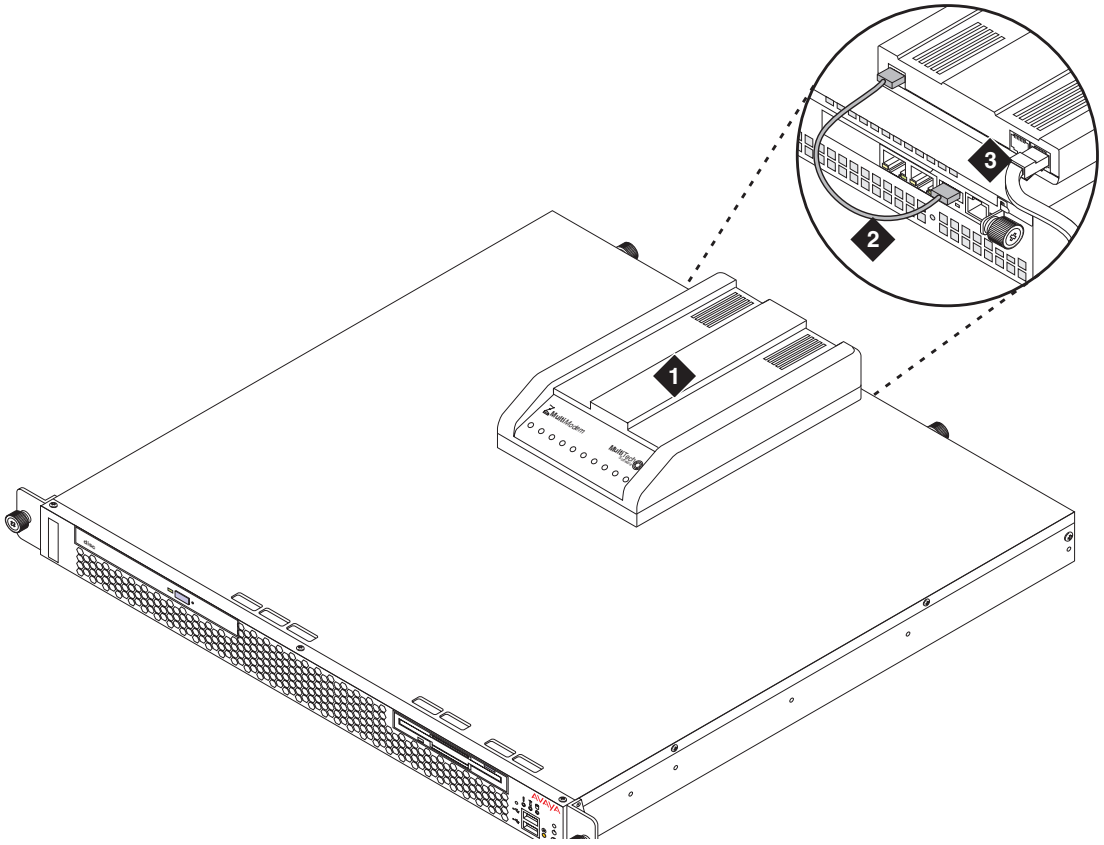


Figure notes:

1. Modem
2. USB cable that connects the USB modem to the USB port on the SAMP
3. Telephone line that connects the modem to the outside line

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 Avaya S8500 Server works with only the Avaya G650 Media Gateway.

In a migration, the server works with the following Avaya media gateways:

- SCC1
- G600
- CMC1

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.

With an S8500 Server, these media gateways can be endpoints that use a Processor Ethernet interface.

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 S8500 Server to allow enhanced flexibility to connect to gateways, endpoints, and adjuncts.

.Table 4 lists the possible uses of the PE interface for an S8500 primary controller.

Table 4: Use of the PE interface for a simplex S8500 primary controller

Possible functions of the PE interface	Status of the function on the S8500 Server	Administration needed?
Registration	The PE interface is enabled for registration on a simplex main server.	No. The Communication Manager software automatically enables the use of the PE interface for registration.
H.248 gateway registration	H.248 gateway registration is allowed on the S8500 main server using the PE interface.	Yes. You perform the administration to allow H.248 registration on the PE interface of the S8500 main server on the ip-interfaces procr form.
H.323 endpoint registration	H.323 registration is allowed on the S8500 main server using the PE interface.	Yes. You perform administration to allow H.323 registration of the PE interface of the S8500 main server on the ip-interfaces procr form.
Adjunct connectivity	Adjunct connectivity is allowed on the S8500 main server using the PE interface.	Yes. To administer adjuncts, you must use the ip-services form or the communication-interface processor-channels form before the survivable-processor form.

About S8500 LSP mode

Starting with Release 3.1 of Communication Manager, you can configure the S8500 as a local survivable processor (LSP), and, the S8500 can be the primary controller for an IP network with port networks. This new functionality is enabled by allowing H.248 gateways and H.323 endpoints to use the Processor Ethernet (PE) interface of the S8500 instead of a C-LAN interface to register with the S8500.

Table 5 lists the possible uses of the PE interface for an S8500 LSP.

Table 5: Use of the PE interface on the S8500 LSP

Possible functions of the PE interface	Status of the function on the LSP server	Administration needed
Registration	The PE interface is always enabled for registration.	No. The Communication Manager software automatically enables the use of the PE interface for registration.
H.248 gateway registration	H.248 gateway registration is enabled by default.	No. The H.248 gateway enabled field on the ip-interface procr form defaults to **yes** on an LSP. To temporarily disable H.248 registration on the LSP, you can change the ip-interfaces procr form on the LSP. Any change that you perform on the LSP is lost when the LSP receives a file sync from the main server. After a file sync H.248 gateway registration will default to **yes**.
H.323 endpoint registration	H.323 endpoint registration is enabled by default.	No. The H.248 gateway enabled field on the ip-interface procr form defaults to **yes** on an LSP. To temporarily disable H.248 registration on the LSP, you can change the ip-interfaces procr form on the LSP. Any change that you perform on the LSP is lost when the LSP receives a file sync from the main server. After a file sync, H.248 gateway registration defaults to **yes**.
Adjunct connectivity	Adjunct connectivity is enabled by default.	Yes. You must perform adjunct administration for the LSP on the main server.

The PE interface on an S8500 LSP supports three adjuncts:

- Call Management System (CMS)
- Application Enablement Services (AESVCS)
- Call Detail Recording (CDR)

The S8500 as a primary controller can connect to gateways and endpoints that use both C-LANs and the PE interface. The traffic over these interfaces can be load balanced.

S8500 LSP license file

The license file for an LSP must have the following attributes:

- The Local Survivable Processor (FEAT_LSP) field is set to **y.**
- A Module ID (MID) that is greater than 1. This value is set by the license file and cannot be administered in Communication Manager.
- A System ID (SID). The SID is unique to the system configuration. The primary controller and all LSPs have the same SID.
- The serial number of an H.248 media gateway to serve as the license serial number host.

  During initial installation, when the LSP server is reset, the LSP sends this serial number to the primary controller. The primary controller then matches the serial number to the serial number of an existing media gateway. The primary controller sends the IP address of the media gateway back to the LSP. To verify the license, the LSP can then contact that media gateway and request the serial number. The LSP compares the serial number from the media gateway with the serial number from the license of the LSP.

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:

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

- The IP address
- The subnet mask
- The gateway IP address
- The trap receiver IP address
- 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 IP addresses for the UPS

The following table shows the default IP addresses for the UPS.

IP address for the UPS	198.152.254.239
Subnet mask for the UPS	255.255.255.0
Gateway address for the UPS	198.152.254.201
IP address for the trap receiver (server)	Customer provided

For how to administer the SNMP module in the UPS, see Administering the SNMP module on page 35.

Prerequisites for configuring the SNMP module

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

- Your Services laptop computer is plugged into the correct administration port on the SNMP module on the UPS.
- The UPS is plugged into a nonswitched electrical outlet.
- 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.

- 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 36.

- 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 55.

Administering the SNMP module

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. Use 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 36.
8. When you finish, disconnect your computer from the UPS.
9. Connect one end of a CAT5 straight-through cable to the RJ45 connector on the UPS 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 S8500 Server* (555-245-701).

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:

- UPS on Battery—Indicates an AC power failure. Based on the level of battery reserve, a shutdown is pending.
- UPS in Bypass—The UPS failed or is overloaded.
- 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:

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:

- The IP address
- The subnet mask
- The gateway IP address
- The trap receiver IP address
- 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

The following table shows the default values for the Ethernet switch.

Parameter	Single control network (CNA)	Duplicated control network (CNB)
IP address for the Ethernet switch	198.152.254.240	198.152.255.240
Subnet mask for the Ethernet switch	255.255.255.0	255.255.255.0
IP address for the trap receiver (server)	Customer provided	Customer provided

For how to administer the SNMP subagent in the Ethernet switch, see Configuring the Ethernet switch on page 38.

Preparing to configure the Ethernet switch

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

- The Ethernet switch power cord is connected to the back of the switch and to the back of a UPS.
- 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.

- 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.

- 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 55.

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 tha.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.

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.

This chapter covers the following tasks:

- Clearing the ARP cache on the laptop on page 41
- Applying power to the server on page 42
- Accessing the server on page 42
- Configuring Telnet for Windows 2000 and Windows XP on page 42
- Installing Communication Manager on page 43

Important:

Follow the installation instructions in this document to install an S8500B Server to run the Expanded Meet-me Conferencing (EMMC) application. Then use the *Expanded Meet-me Conferencing (EMMC) version 1.0 Installation and Troubleshooting Guide*, (04-300527) to complete the installation of the EMMC. The two CD-ROMs *EMMC Software Disk 1* and *EMMC Software Disk 2* contain the EMMC software.

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 immediately after you turn on the power to the server.

1. Connect the AC power cord to the server and to the UPS or a nonswitched electrical outlet.
2. If the server does not turn on, press the white power control button on the front of the server (for S8500C see Figure 1: S8500C front panel on page 16and for S8500B see Figure 3: S8500B front panel on page 17).
3. Immediately place the Communication Manager CD-ROM into the CD-ROM drive on the server. Or, If you are installing an S8500 Server to run the Expanded Meet-me Conferencing (EMMC) application, use the CD-ROM that is labeled *EMMC Software Disk 1*.

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

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. On the **Select Messaging Options** screen, select **<OK>** if you want to install Communication Manager Messaging (CMM) concurrently with Communication Manager. Select **No** if you do not.

Note:

Starting with Communication Manager release 5.2, IA 770 is called Communication Manager Messaging.

Note:

If you do not install CMM concurrently with Communication Manager at this time, and decide later to install it, you must reinstall Communication Manager.

6. The program starts the installation and displays the progress. This process takes approximately 20 minutes to complete. 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.
7. After the reboot, perform one of the following actions:
   - If you are installing the S8500 Server as a main server, continue with the next section of this document.
   - If your are installing the S8500 as an LSP, continue with Installing and configuring an S8500 Server as an LSP on page 76.
   - If your are installing the S8500 as an ESS, see the *Using Avaya Enterprise Survivable Server (ESS)* guide.
   - If you are installing an S8500 Server to run the Expanded Meet-me Conferencing (EMMC) application, you are finished with this document. Continue the EMMC installation procedures described in *Installing and Troubleshooting the Expanded Meet-me Conferencing (EMMC)* (04-300527).

Chapter 4: Server configuration

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

This section covers the following tasks:

- Creating a super-user login on page 46
- Installing the license and authentication files on page 47
- Configuring the server manually on page 48
- Running the Avaya Installation Wizard on page 53
- Verifying the RMB IP information on page 53
- Upgrading the SAMP firmware on page 54
- Verifying the server connection to the customer LAN (if provided) on page 54
- Enabling firewall settings on page 55
- Enabling network time servers on page 56

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 143.

Methods of Configuring a server

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

1. Configuring the server manually on page 48 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 SAMP update files from the Services laptop to the server. For how to open the System Management Interface, see Accessing the System Management Interface on page 141.

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**.

Copying license and authentication files to the server

1. Log on to the System Management Interface and click **Administration > Server (Maintenance) > Download Files.**
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the Choose File window on your computer. Find the files that you need to copy to the server.
4. Click **Download** to copy the lilcense and the authorization files to the server.

The files are automatically copied to the default file location /var/home/ftp/pub.

Installing the license and authentication files

This section describes the procedure to install the license file and the Avaya authentication file on the active S8500 server.

Installing the license file

1. Log on to the System Management Interafce and click **Administration > Server (Maintenance) > License File**. The system displays the License File Web page.
2. Do one of the following:
   - If you have already downloaded the file to this server, select **Install the license file I previously downloaded**.
   - If you have not downloaded the file to this server, select **Install the license file specified below**, and perform one of the following steps:
     - In the File Path box, browse to the directory where the license file is located.
     - 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. Log on to the System Management Interface and click **Administration > Server (Maintenance) > Authentication File**. The system displays the Authentication File Web page.
2. Perform one of the following tasks:
   - Select **Install the Authentication file I previously downloaded**, if you already downloaded the file to this server.
   - 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.

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 47.

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 49.

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: S8500 configuration Web pages

Page	S8500 Main	S8500 ESS	S8500 LSP
Server Role	✓	✓	✓
Set Identities	✓	✓	✓
Configure Interfaces	✓	✓	✓
Configure ESS	✓	✓	✓
Configure LSP	✓	✓	✓
Configure UPS	✓	✓	NA
Set DNS/DHCP	✓	✓	✓
Set Static Routes	✓	✓	✓
Configure Time Server	✓	✓	✓
Set Modem Interface	✓	✓	✓
Configure RMB	✓	✓	✓

The following describes each of the configuration pages:

- **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.
- **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 51 for a guide to assigning functions to Ethernet interfaces.
- **Configure Interfaces** — Use this page to enter the IP address, subnet mask, gateway, and speed for the management LAN and control network.
- *(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).
- **Configure LSP** — Use this page to configure the server as a Local Survivable Server (LSP).
- **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.
- **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.
- **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**.
- **Configure Time Server** — Use this page to specify the time source that the Avaya server uses to set the time of day.
- **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.
- **Configure RMB** — Use this page to configure the remote maintenance board (RMB).

Ethernet interface assignments

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

Table 7: S8500-Series Server Ethernet assignments

	S8500-Series Main or ESS to S8500 dedicated control	S8500-Series Main or ESS to S8500 non-dedicated control	S8500-Series ESS to S8700-series Server, dedicated control	S8500-Series ESS to S8700-series Server, non-dedicated control
Control network A	eth0	eth0	eth0 (if used)	eth0 (if used)
Control network B	not used	not used	eth3 (if used)	eth3 (if used)
LAN	eth4	eth0	eth4	eth0
Processor Ethernet (PE)	eth0	eth0	eth0 (if used)	eth0 (if used)

For information on mapping to the physical ports, see Figure 7: S8500C Server connectivity guide on page 25 or Figure 8: S8500B Server connectivity guide on page 26.

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 LSP
   - Configure Switches
   - Set DNS/DHCP

- Set Static Routes
- Configure Time Server
- Set Modem Interface
- Configure RMB
- 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 48 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:

- Set the date, the time, and the time zone
- Configure the server
- Configure the Remote Maintenance Board (SAMP)
- 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.

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

To use the Installation Wizard, you can either:

- 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.
- 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.

   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 49.

Verifying the RMB IP information

The Remote Maintenance Board (RMB) page is under **Optional Services** in the Installation Wizard configuration process. Verify that the Installation Wizard retrieved the IP information from the EPW. If the information is not there, complete all fields manually.

To allow Services access to the remote maintenance board through a cross-over cable, verify the information in the following fields:

- **IP Address 192.11.13.6**
- **Subnet Mask 255.255.255.252**

If the information is not there, complete the fields manually.

Upgrading the SAMP firmware

You might need to update the SAMP firmware if the most current version is not installed. Information about the versions that require updates should be included in your project planning information.

For how to update SAMP software, see *Using the Avaya Server Availability Management Processor (SAMP).*

1. Check the firmware version:
   a. Use SSH to access the server and log in.
   b. Type **`sampcmd samp-update status`** and press **Enter**.
   c. Check the firmware version displayed.
2. If you need to update the firmware, on the Server Administration Interface under Miscellaneous, click **Download Files**.
3. Enter the information to copy the firmware file to the server.
4. Use SSH to access the server and log in.
5. To start the update process, type **`sampupdate`** and press Enter.

   The update process takes approximately 5 minutes.

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

1. Log on to the System Management Interface and click **Administration > Server (Maintenance) > 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.
8. Click **Close Window**.

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. Log on to the System Management Interface and click **Administration > Server (Maintenance) > 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 52.

For more information about NTP, see RFC 958.

Checking LED activity on the dual NIC

When the S8500 Server is in service, check the LEDs on each port of the dual network interface card (NIC) for connection and activity. Ensure that the LED on the left that indicates connection is lit and the LED on the right that indicates activity is lit or blinking. For dual-NIC LED information, see Figure 10: S8500B rear panel dual-NIC LEDs on page 58.

Note:

The dual NIC is optional with the S8500B but ships installed with the S8500C. The dual NIC is located on the rear panel in different positions on the S8500B and S8500C but the port LEDs are the same. For a diagram of the S8500C back panel, see Figure 2: S8500C back panel.

Figure 10: S8500B rear panel dual-NIC LEDs

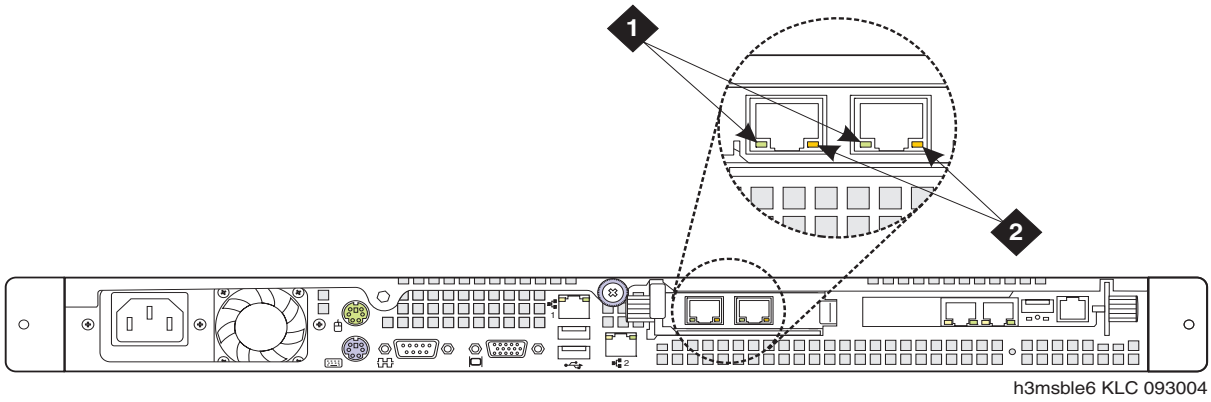


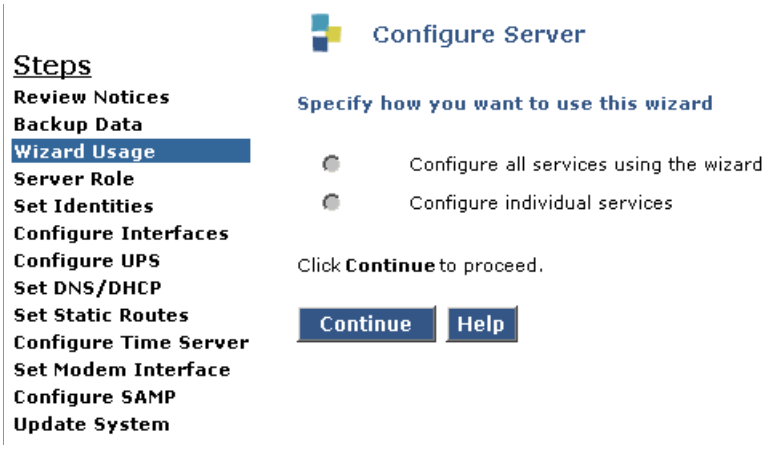
Figure notes:

1. Network activity LED (TX/RX)
2. Connection rate:
   – Off: a 10BaseT active link
   – Green: a 100BaseT active link
   – Orange: a 1000BaseT active link

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. The following table shows the default assignments for three S8500 configurations:

Table 8: Recommended port assignments for S8500B and S8500C[1]

Functionality	S8500B with dual NIC	S8500B without dual NIC	S8500C
Control Network A	Ethernet 0	Ethernet 0	Ethernet 0
Services laptop computer	Ethernet 1	Ethernet 1	Ethernet 1
Internal SAMP	Ethernet 2	Ethernet 2	Ethernet 2
Control Network B — ESS for S87xx system with duplicated control	Ethernet 3	Unused	Ethernet 3
Corporate LAN — Private control network	Ethernet 4	NA	Ethernet 4
Corporate LAN — Shared control network	Ethernet 0	Ethernet 0	Ethernet 0

1. These port assignments are recommended when using the Set Identities Web page in the System Management Interface. The settings entered on this Web page might not correspond to the setting reported for the CLI `ifconfig` command.
2. Ethernet 2 is internal to the S8500 Server and is not configurable.

6. Click **Continue**.
7. Complete the following information for Ethernet 2:
   - IP address
   - Gateway
   - Subnet mask
   - Speed
8. Verify with the network administrator that the LAN hardware supports 802.1q priority tagging. If supported, select **VLAN 802.1q priority tagging**.
9. 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.

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

Chapter 5: IP interface configuration

This chapter covers the following tasks:

- Connecting to the IPSIs on page 61
- IPSI address configuration on page 61
- Programming the IPSI for static addressing on page 62
- Setting the VLAN and diffserv parameters on page 65
- Programming the IPSI for DHCP addressing on page 66

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.

For how to connect the S8500 Ethernet cables, see About server port connections on page 25.

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:

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

Note:

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:

- Programming the IPSI for static addressing on page 62
- Programming the IPSI for DHCP addressing on page 66

Programming the IPSI for static addressing

Important:

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 11.

Figure 11: Connecting the laptop directly to the IPSI

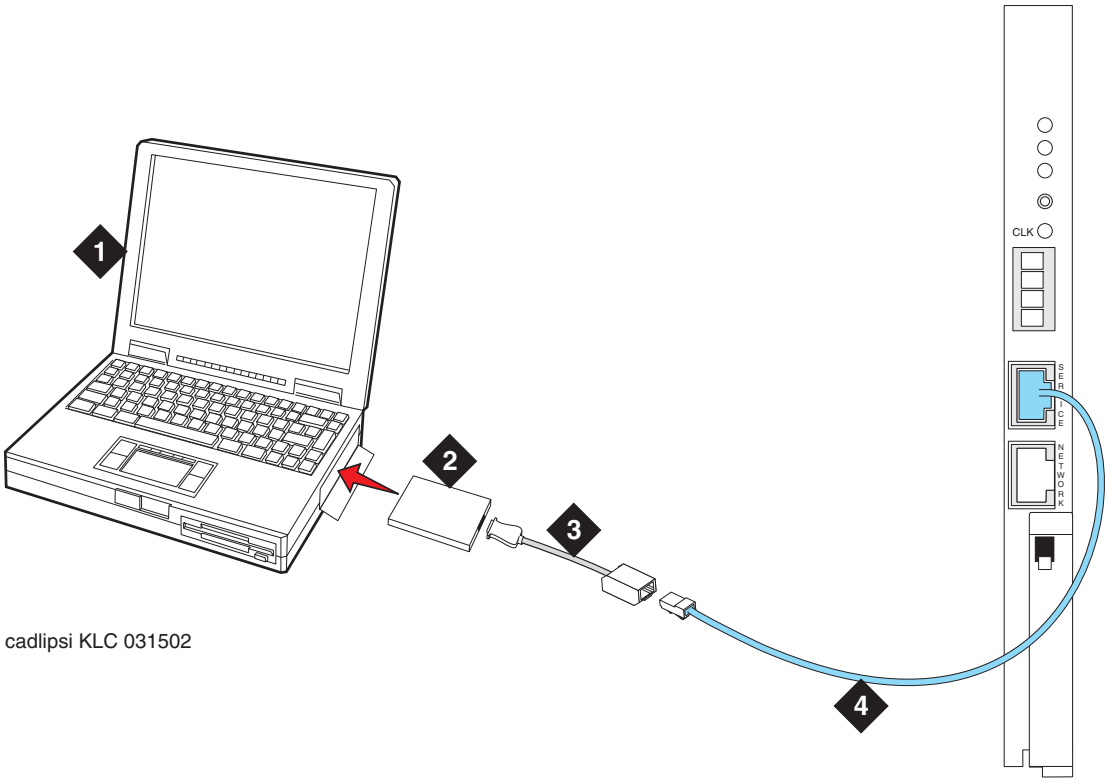


Figure notes:

1. Services laptop computer
2. PCMCIA Network Interface Card (NIC)
3. NIC adapter cable (if necessary)
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 135.

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 12).

Figure 12: IPSI LED display for static address

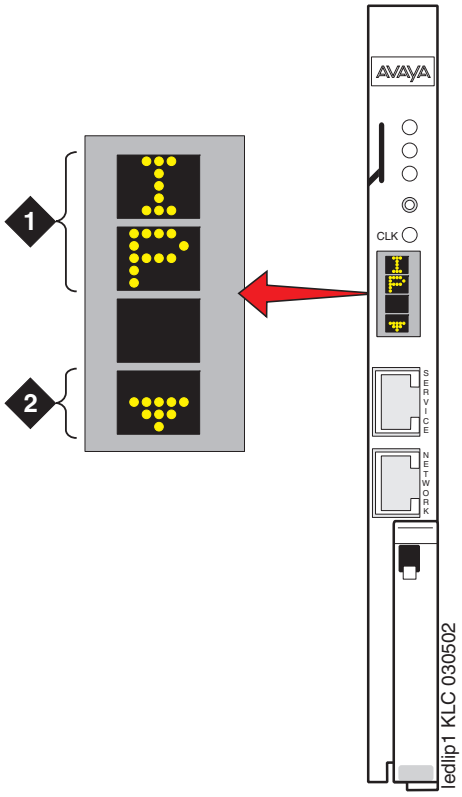


Figure notes:

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:

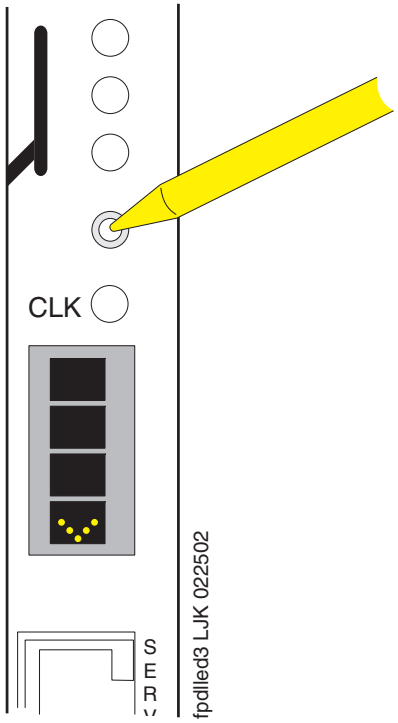
In the following procedure, you must start step 2 within 5 seconds after inserting the circuit pack.

1. Fully insert the TN2312BP IPSI circuit pack. If necessary, reseat 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 reseat, the circuit pack and start again.

Note:

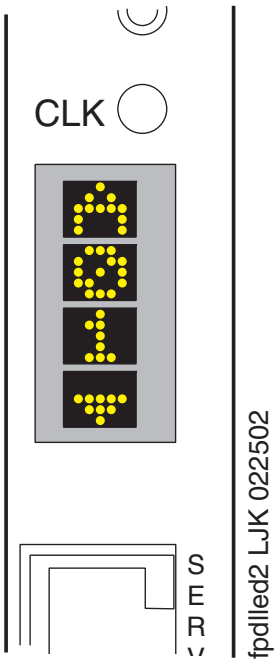
If you have only one system, the default switch ID is A. The second system is B and so on. The switch ID is *not* the media gateway or carrier letter.

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 v is shown in the fourth or bottom character. When the DHCP server assigns an address to the IPSI, the center of the v fills in. The filled in v looks like the bottom half of a diamond.



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

Chapter 6: 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 69
- Adding media gateways on page 70
- Enabling the IPSI on page 71
- Adding the IPSI to the system on page 72
- Setting the alarm activation level on page 72
- Saving translations on page 73
- Verifying connectivity to the server on page 73
- Verifying that the IPSIs are translated on page 73
- Upgrading the IPSI firmware version (if necessary) on page 73
- Enabling control of the IPSIs on page 74
- Verifying the license status on page 74

Inputting initial system translations

1. Open a SAT session. See Accessing the SAT on page 142.
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 the **IP Server Interface System Parameters** screen, verify that the primary control subnetwork address is 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 **Control Subnet Address** field is incorrect, use the System Management Interface to change the server configuration to match the Server IP address in **configure server**. From the Installation menu, 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. In the **Host** field, enter the IP address for the IPSI that is listed in the **Location** field.

```
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.

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

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. Log on to the System Management Interface and click **Administration > Server (Maintenance) > 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. 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

Log on to the System Management Interface and click **Administration > Server (Maintenance) > License File** and verify that the license mode is now normal.

Chapter 7: S8500 Server Roles

Configuring an S8500 server as a main server

To configure a server as a main server in a gateway-only configuration, follow these steps:

1. Log on to the System Management Interface. From the Installation menu, click **Configure Server**. The system displays the Configure Server wizard.
2. Click **Continue** until you get to the Specify how do you want to use this wizard page.
3. Select the **Configure individual services** and click **Continue**. The system displays the Review Notices page.
4. On the left navigation menu, click **Server Role**. The system displays the Specify Server Role page.
5. Select **a main server** and click **Change**. After a successful completion, the system displays `Updating System Files` message.
6. On the left navigation menu, click **Set Identities**. The system displays the Set Identities page.
   Use this page to assign Avaya server host names and to assign server functions. The options are pre populated with defaults, but should be changed as needed for the customer's configuration. If no port network is being used, then perform the following steps.
   - In the Control Network A field, select the default **Ethernet 0**.
   - In the Services Port field, select the default **Ethernet 1**.
   - In the Corporate LAN field, select the default **Ethernet 0**.
   - In the Assign the Processor Ethernet to an Interface field, select a suitable option.

   Note:
   Internal RMB Port is set to **Ethernet 2** by default.
7. Click **Continue**. The system displays the Configure Interfaces page.
8. In the Configure Interfaces page, specify the IP address, subnet mask, gateway, and speed for the management LAN and control network.
9. Click **Change**. After successful configuration of ethernet interface, the system displays a message. This completes the procedure to configure a server as a main server. However, you may want to configure the following from the left navigation menu—
   - Configure UPS
   - Set DNS/DHCP

- Set Static Routes
- Configure Time Server
- Set Modem Interface
- Configure RMB

Installing and configuring an S8500 Server as an LSP

Note:
If you are installing the S8500 Server as a primary controller, skip this section.

Starting with Release 3.1 of Communication Manager, the Processor Ethernet (PE) interface is supported on the S8500 Server. The PE interface enables the S8500 Server to operate in Local Survivable Processor (LSP) mode. The PE interface also enables the server to be the primary controller in an IP configuration with no port networks.

For how to administer PE, see *Administering Avaya Aura™ Communication Manager* (03-300509).

To install a new S8500 Server as an LSP, first complete the tasks in *Quick Start for Hardware Installation: Avaya S8500 Server*. Then complete the tasks in the previous sections of this document to:

- Install the S8500 Server hardware in the 19-inch rack
- Connect the cables between the server and the network of the customer
- Connect the SAMP card and the modem
- Configure SNMP and the Ethernet switch
- Install Communication Manager
- Configure the S8500 Server

When you have completed these tasks, proceed with tasks in this section.

1. Copying license and authentication files to the server on page 47.
2. Creating a super-user login on page 46.
3. Configuring the server manually on page 48.
4. Upgrading the SAMP firmware on page 54.
5. Configuring the modem on page 55.
6. Enabling network time servers on page 56.
7. Configuring the server as an LSP on page 77.

Configuring the server as an LSP

Note:
Do not install the license file and the authentication file until you administer the primary controller. For more information, see Administering the primary controller on page 78.

1. Open the Server Administration Interface and from the **Installation** menu, click **Configure Server**.
2. Select **Set Date and Time Zone**. You must set the time of the LSP to the same time zone as the primary controller even if the LSP is physically located in a different time zone.
3. Click **Continue** until you get to the How do you want to use the Wizard page.
4. Select the **Configure Individual Services**.
5. Select **Set Identities**
   - Enter the host name for the LSP.
   - In the **ID** field, check the Server ID (SVID) value. The primary controller is set to SVID 1. If the primary controller is a duplicated S8700-series Server, the server IDs are SVID 1 and SVID 2. The ID for an LSP must be greater than 2 and less than or equal to 256. Gaps in the numbering are allowed. For example, SVIDs can be 10, 20, 30, and so on.
   - In the Control Network A field, select the default **Ethernet 0.**
   - In the Services Port field, select the default **Ethernet 1**.
   - In the Corporate LAN field, select the default **Ethernet 0**.
   - In the Control Network B field, select the default **unused**.
   - In the Assign a Processor Ethernet Interface field, select **Corporate LAN**.
6. Click **Continue**.
7. On the Configure Interfaces Web page, enter the following IP addresses:
   - In the **IP address server1** field, enter the IP address for the LSP.
   - In the **Gateway** field, enter the IP address for the LAN gateway.
   - In the **Subnet mask** field, enter the subnet mask for the LSP.
8. In the **Speed** field, select **Autosense**.
9. Click **Change**.
10. From the list in the left margin, select **Configure LSP/ESS**.
    - Select **This is a local survivable processor (LSP)**.

- In the **Registration address** field, enter the IP address of a C-LAN that is administered and enabled in the translations of the primary controller. If the primary controller is an S8500 Server, this address can be the IP address of the Processor Ethernet of the primary controller.
- In the **File Synchronization address at the main cluster** field, enter the physical IP address or addresses of the primary controller servers. These addresses *must* be connected to the corporate LAN. The IP address *cannot* be the address of a port that is assigned to a control network if the control network is dedicated to the IPSI connection. If the control network or the control networks are dedicated, enter the IP address of the port that is assigned to the corporate LAN.

11. Click **Change** to save your changes.

Administering the primary controller

You must administer the primary controller so that the controller can identify and communicate with the S8500 LSP.

1. At the SAT command line, type **`change node-names ip name`** and press **Enter**, where ***`name`*** is the name of the LSP.
2. In the **Name** column, type the name of the LSP.
3. In the **IP Address** column, type the IP address of the LSP.
4. At the SAT command line, type **`add survivable-processor name`** and press **Enter**, where ***`name`*** is the LSP name from the Node Names screen.

   The system displays the Survivable Processor screen.

```
add survivable-processor sv-mg2-lsp                          Page   1 of  xx

                SURVIVABLE PROCESSOR - PROCESSOR ETHERNET

                          Node Name: sv-mg2-lsp
                         IP Address: 128.256.173.101
                               Type: LSP

                     Network Region: 1
```

5. The Type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
6. Enter a network region for the LSP. The default is **1**. However, a different network region might be better suited for the LSP to provide media gateway and IP telephone support.
7. On pages 2 and 3 of the screen, add any adjuncts that the LSP can support if a failover from the primary controller occurs.

For how to administer the Survivable Processor form, see *Administrator Guide for Avaya Aura™ Communication Manager* (03-300509).

Enabling license server capability on a media gateway

If a G250/G350/G450 Media Gateway provides the serial number, access the *administration level* command line of the media gateway and run the command **ip license-server**. If a G700 Media Gateway provides the serial number for the S8500 LSP license, skip this step and continue with Installing and verifying the license on the new LSP on page 79.

Note:
The gateway that provides the serial number must be connected to the LSP such that it remains connected in the event of a network failure.

Installing and verifying the license on the new LSP

On the S8500 LSP, install a new license file with the appropriate settings for an LSP server.

To install the license file and the authentication file, complete the following steps:

1. On the Server Administration Interface, under Security, click **License File**.
2. On the License File Web page, click **Restart CM**.

   Important:
   After installing the license file, the system displays a message that warns you that the license requires a restart. Do *not* restart the server at this time.
3. Under Security, click **Authentication File**.
4. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system tells you the authentication is installed successfully.
5. Restart Communication Manager to sync the license for LSP status.
   a. Access the server command line interface using an SSH client, like PuTTY, and an IP address of 192.11.13.6.
   b. Type `stop -caf`
   c. Type `start -caf`
6. To verify that the S8500 Server that you are installing is licensed as an LSP:

Note:
When you access the SAT screen before you reset the system, the screen might indicate "License mode not available." This problem is resolved after the reset.

a. Open a SAT session on the LSP and type **`display system-parameters customer-options`** and press **Enter**.

b. On the System-Parameters Customer-Options form, verify that the Local Survivable Processor field is set to **y** and verify that the Processor Ethernet field is set to **y**.

Opening the TCP ports on the S8500 LSP

You can open various TCP ports for Processor Ethernet (PE) on the firewall to enable the connections to work for the LSP.

1. On the Server Administration Interface, under Security, click **Firewall**.

   The system displays the Firewall Web page.

   Note:
   The ftp, telnet, and tftp services are not required.

2. In the Input to Server column, ensure that the check box for **snmp** is selected.
3. Click **Advanced Setting**.

   The system displays the Advanced Firewall Settings Web page.
4. Verify that the following defaults are set:
   - **Output to server** is selected for **gateway compatibility**, ports **1024:65535**
   - **Input to server** is selected for **ip-signaling-1**, ports **5000:5021/tcp**
   - **Input to server** is selected for **ip-signaling-2**, ports **5024:9999/tcp**
   - **Input to server** is selected for **h248message**, port **2945/tcp**
   - **Input to server** *and* **Output to server** is selected for **filesync**, port **21874/tcp**
   - **Input to server** *and* **Output to server** is selected for **h323gatestat**, port **1719/udp**
   - **Input to server** *and* **Output to server** is selected for **h323hostcall**, port **1720/tcp**

   If any of the defaults are set incorrectly, contact your sales representative.
5. Click **Standard Service** to return to the first Firewall page, and then click **Submit**.

Resetting the S8500 LSP

Use the reset command to notify all processes of the new parameters:

Note:
When you access the SAT screen before you reset the system, the screen might indicate a license mismatch. This problem is resolved after the reset.

From the SAT command line, type **`reset system 4`** and press **Enter**.

The system resets. The system also registers with the primary controller and receives the translations from the primary controller.

Verifying that the primary controller identifies the new LSP

1. Wait several minutes after you reset the S8500 LSP. On the primary controller, run the SAT command **`list survivable-processor`** to verify that the LSP server registers, and that translations are updated.
2. If the LSP is registered, the Service State? field shows `in-service` and the Translations Updated field shows the time and the date of the update.

```
list survivable-processor                                        Page   1 of  xx
                          SURVIVABLE PROCESSORS
 Name            Type      IP Address     Reg Act          Translations     Net
                                                           Updated          Rgn

 svs8300c-14     LSP       10.13.2.57      n                                1
 svs8300c-16     LSP       10.13.2.12      y   n          3:05 4/13/2009    1
 svs8510-7       ESS S     10.13.2.45      n                                1
 svs8720-1       ESS D     10.13.1.145     n                                1
```

Readministering media gateways to point to the LSP

Change the controller list for each G700, G350, or G250 Media Gateway that uses the LSP as an alternate controller. This change enables the media gateway to seek service from the LSP if the connection to the primary controller fails.

For how to change the controller list of the media gateway, see one of the following documents:

- *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Server*, 555-234-100
- *Installation and Upgrades for the Avaya G250 Media Gateways*, 03-300434
- *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394

Chapter 7: Postinstallation administration

This section covers the following tasks:

- Verifying translations on page 83
- Setting rules for daylight savings time on page 84
- Setting locations (if necessary) on page 85
- Verifying the date and the time (main server only) on page 86
- Clearing and resolving alarms on page 87
- Backing up files to the compact flash media on page 90
- Enabling alarms to INADS by way of a modem on page 89
- Enabling alarms to INADS by way of the SNMP module on page 90
- Before leaving the site on page 91

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                                          Page   1 of   5
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Number  Name              Timezone  Daylight-Savings        Number Plan
                            Offset   Rule                    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 49.

4. Repeat this procedure, beginning with step 1.
5. Verify that the Daylight Savings Rule field is correct.
   - 0 if this server is in a location that does not use daylight savings time

- 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 84.

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 85.

Clearing and resolving alarms

1. Log on to the System Management Interface and click **Administration > Server (Maintenance) > Current Alarms**.

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

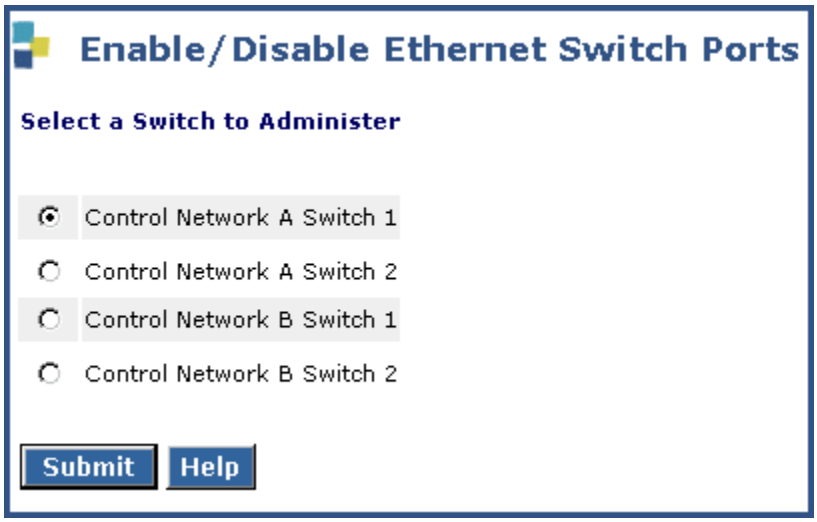
2. Select the server alarms to clear and click **Clear**.

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

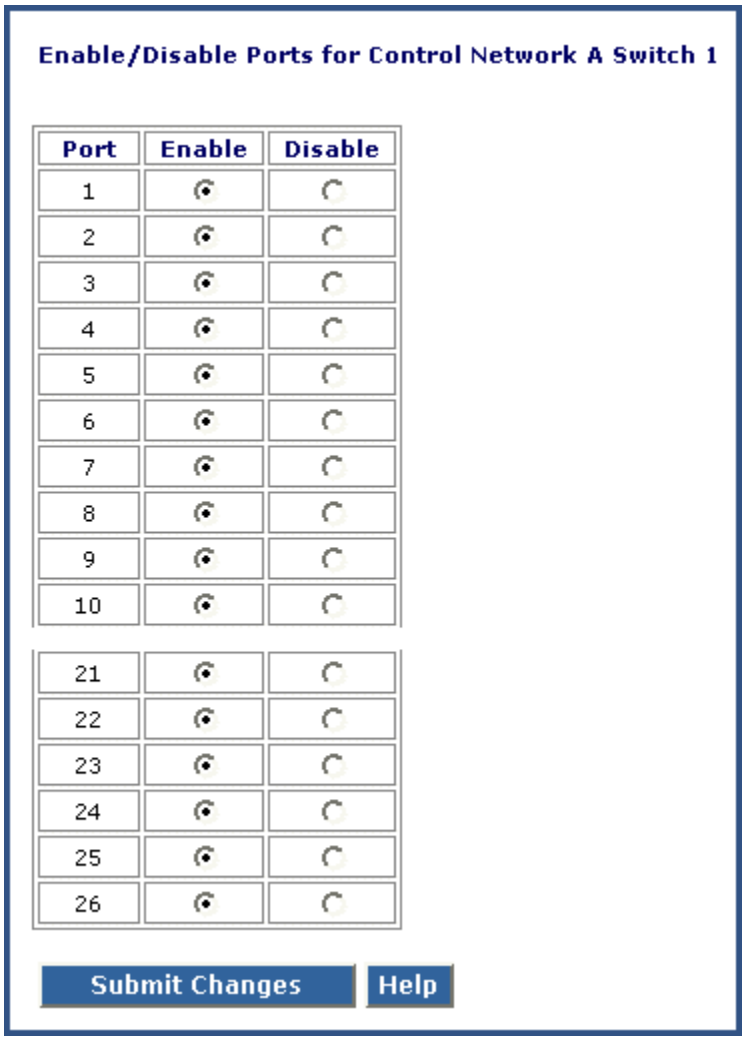
Enabling and disabling the Ethernet switch ports

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**.



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



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

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 front of the server.
2. Insert the compact flash media into the top right slot of the drive.
3. Log on to the System Management Interface and click **Administration > Server (Maintenance) > 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. For more information on LED display, see S8500 front-panel LEDs on page 95.

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

Before leaving the site

- Provide the default LAN security settings to the customer.
- 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:

- Testing the IPSI circuit packs
- Testing the license file
- 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.

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.

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.

S8500 LEDs

The Avaya S8500 Servers have five or six LEDs on the front and four LEDs on the back. The S8500B and S8500C have the same LEDs but in different locations. The S8500B can have an additional LED indicating activity on the optional floppy disk drive. The S8500C does not support a floppy disk drive.

The SAMP module has two LEDs under each of the Ethernet connections, one for transmission activity and another for transmission speed.

Figure 13: S8500C front panel on page 94 and Figure 14: S8500C back panel on page 95 show the locations of the front-panel LEDs on the S8500C and S8500B.

Figure 13: S8500C front panel

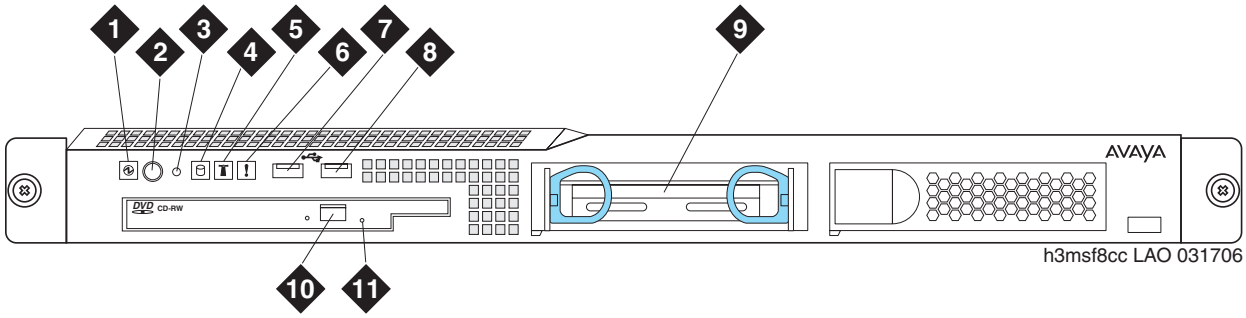


Figure notes:

1. Power-on LED
2. Power button
3. Reset button
4. Hard disk drive activity LED
5. Locator LED
6. System error LED
7. USB port
8. USB port
9. Hard disk drive
10. CD eject button
11. CD-ROM drive activity LED

Figure 14: S8500C back panel

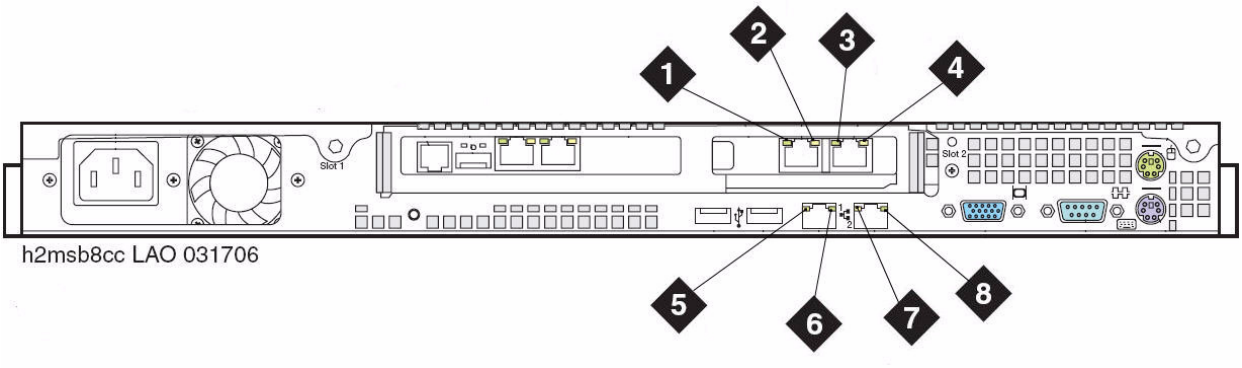


Figure 15: S8500B front panel

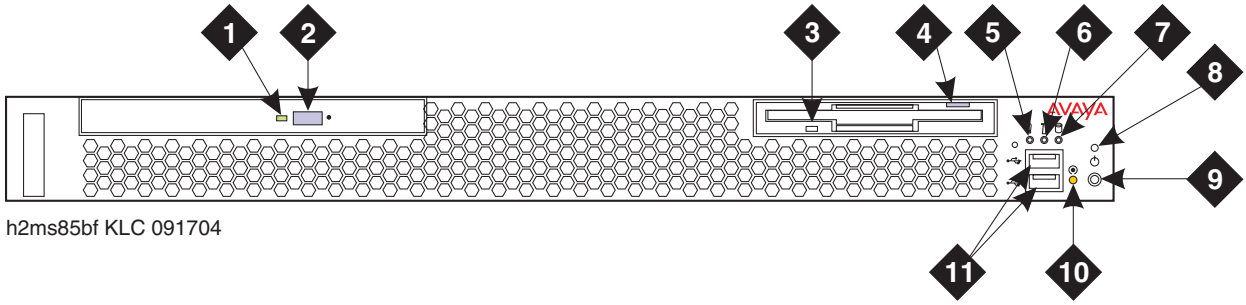


Figure notes:

1. CD-ROM drive activity LED
2. CD-ROM eject button
3. Diskette drive activity LED
4. Diskette eject button
5. System error LED
6. System locator LED.
7. Hard disk drive activity LED
8. Power on LED
9. Power control button
10. Reset button — Press to reset the server and run the power-on self-test (POST).
11. USB connections for the compact flash drive.

The functions of the front-panel LEDs are as follows:

Table 9: S8500 front-panel LEDs

LED	Description
Power on	When lit and not flashing, the server is turned on. When flashing, the server is turned off and still connected to the AC power source. When off, AC power is not present, or the power supply or the LED failed.
Hard disk drive	When on or blinking, indicates HDD activity.

Table 9: S8500 front-panel LEDs

LED	Description
Locator	Use this blue LED to locate the server if the server is in a location with numerous other servers.
System error	When on, indicates a system error.
CD-ROM drive	When on or blinking, indicates activity on the CD-ROM drive.
Floppy disk drive (S8500B only)	When on or blinking, indicates activity on the FDD drive.

Figure 16: Rear view of S8500B Server on page 96 shows the Ethernet port LEDs on the back panel of the S8500B. Each port connector has two LEDs, one for transmission activity and one to indicate the transmission speed. The port LEDs on the S8500C are the same as on the S8500B.

Figure 16: Rear view of S8500B Server

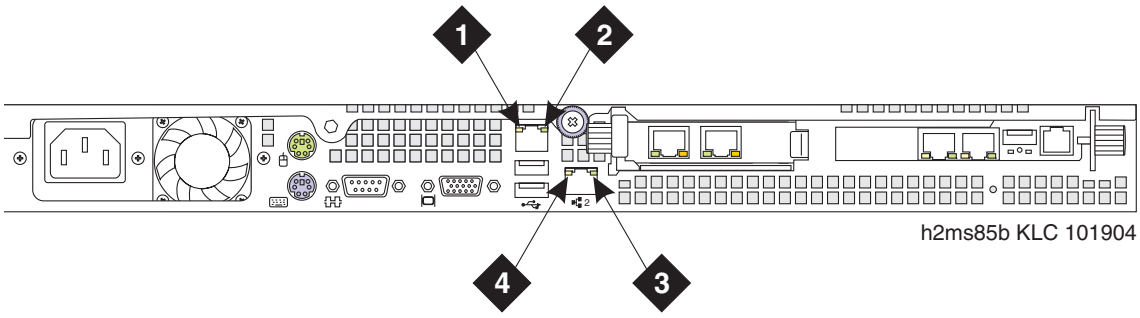


Figure notes:

1. Speed 1 Gbps LED on Eth 0. **4.** Speed 1 Gbps LED on Eth 1.	When lit, these LEDs indicate that the Ethernet network speed is 1 Gbps. When off, these LEDs indicate that the Ethernet network speed is 10 Mbps or 100 Mbps.
2. Transmit/receive activity LED on Eth 0. **3.** Transmit/receive activity LED on Eth 1.	When lit, these LEDs indicate activity between the server and the network.

Note:

On the S8500C, the Ethernet ports are located below the dual NIC but the port LEDs have the same location and function as shown in Figure 16. See Figure 2: S8500C back panel on page 17.

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:

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

The front panel of the C360-Series switches has:

- One port LED that is associated with each port
- Three system status LEDs
- 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 17: LEDs on the Powerware 9125 UPS

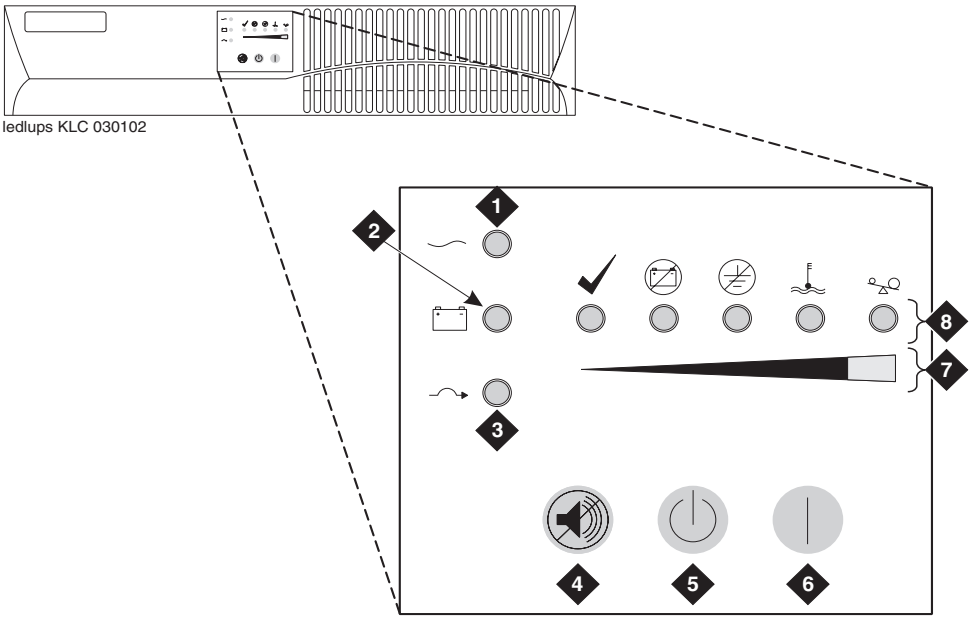


Figure notes:

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

TN2312BP IPSI LEDs

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

- Standard LEDs and connector slots
- 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 19: IPSI LED display for a static IP address on page 102)
  - Connectivity . If SIPI has connectivity and an IP, the LED panel shows a solid downward pointing triangle (see Figure 19).

For more information on troubleshooting the configuration of the server harware, see Appendix B: Installation troubleshooting on page 145.

Figure 18: TN2312BP IPSI circuit pack faceplate

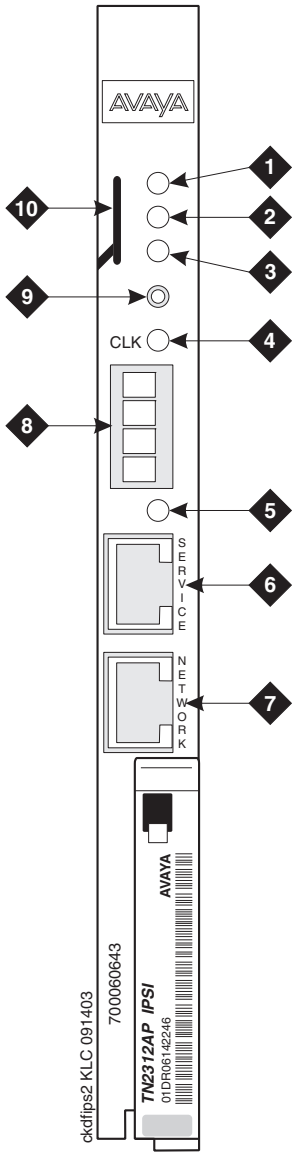


Figure notes:

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

Figure 19: IPSI LED display for a static IP address

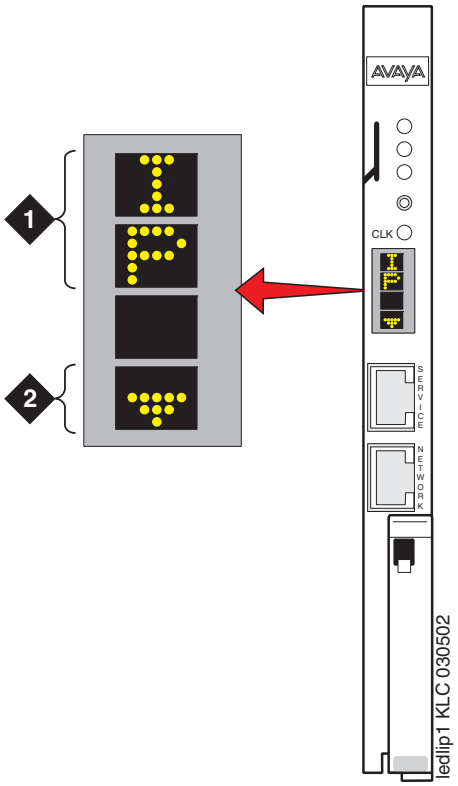
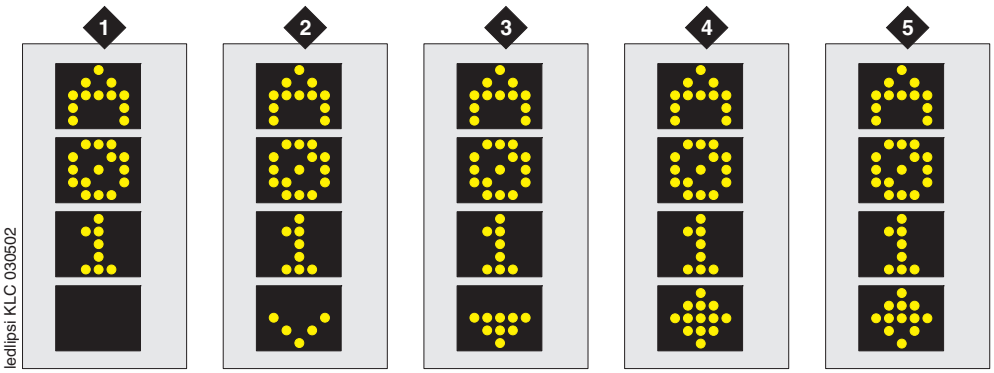


Figure notes:

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

Figure 20: 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

Chapter 9: Installing the Avaya S8510 Server Family and its Components

Overview of server and components

This server uses the Linux operating system and supports several Avaya software applications. It is generally used in simplex mode, but for some products it is duplicated.

Server components

The server comes with the following components.

- One or two Quad Core Intel® Xeon® Processor 5000 Sequence.
- A minimum of 2 GB (2 x 1 GB) of 667 MHz (when available), fully buffered DIMMs (FBD), upgradable to a maximum of 32 GB by installing combinations of 1-GB, 2-GB, or 4-GB memory modules in the eight memory module sockets on the system board.

The server also features redundant memory, which provides memory sparing or memory mirroring. Either feature is available if 8 identical memory modules are installed.

- Two 3.5-inch, internal hot-pluggable SATA (7200 rpm) hard drives.
- A slimline DVD-ROM/CD-RW drive.
- One hot-pluggable, 670-W power supply with an option of installing a second power supply in a 1 + 1 redundant configuration.
- Four fan modules, each comprises two dual-rotor fans, for a total of eight cooling fans.

The server board includes the following features:

- Two integrated gigabit Ethernet NICs capable of supporting 10-Mbps, 100-Mbps, and 1000-Mbps data rates.
- One dual network interface card (NIC) with gigabit Ethernet NICs capable of supporting 10-Mbps, 100-Mbps, and 1000-Mbps data rates (optional).
- One PCI-e Server Availability Management Processor (SAMP) card (optional)
- An integrated VGA-compatible video subsystem with an ATI ES1000, 33-MHz PCI video controller.

- Back-panel connectors include serial, video, two USB connectors, and two NIC connectors.
- Front-panel connectors include a video and two USB connectors.
- Front-panel 1x5 LCD for system ID and error messaging.

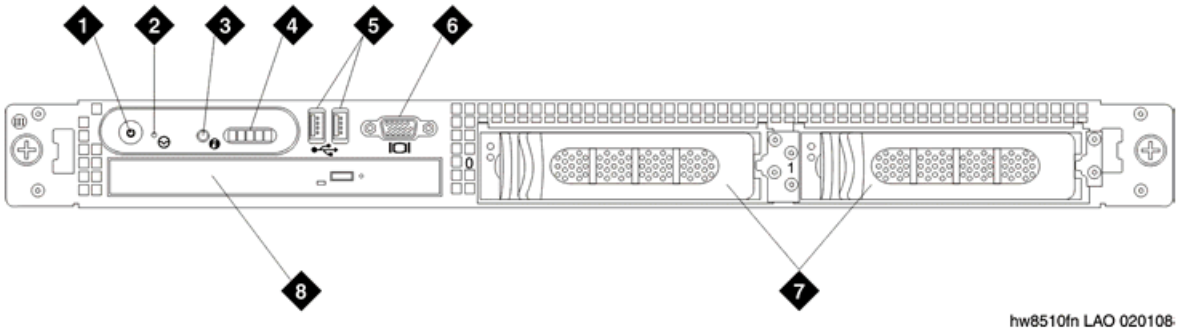
Specifications

Type	Description
Memory	Architecture: PC2–4100 667–MHz fully buffered DIMMS with ECC protection Module sockets: 8 240–pin Module capacities: 1 GB, 2 GB, 4 GB Min/Max RAM: 1 GB/32 GB
Connectors (front)	USB: 2 4–pin, USB 2.0–compliant Video: 15–pin VGA
Connectors (back)	NIC: 2 RJ-45 Serial: 9–pin, DTE, 16550–compatible USB: 2 4–pin, USB 2.0–compliant Video: 15–pin VGA
AC power supply	Wattage: 670 W Voltage:90–264 VAC, autoranging, 47–63 Hz, 10–.0 A (at 90 VAC) Heat dissipation: 2697 BTU/h (maximum) Maximum inrush current: Under typical line conditions and over the entire system ambient operating range, the inrush current may reach 55 A per power supply for 10 ms or less.
System battery	CR 2032 3.0–V lithium ion coin cell
Dimensions (HxWxD/Us)	1.7 x 10 x 30 in. (4.3 x 48.3 x 7./26 cm)/1 U
Weight	39 lb (18 kg)

Environmental specifications

Operating temperature	10° to 35° C (50° to 95° F)
Storage temperature	–40° to 65° C (–40° to 149° F)
Operating relative humidity	8% to 85% (noncondensing) with a maximum humidity gradation of 10% per hour
Storage relative humidity	5% to 95% (noncondensing)
Operating maximum vibration	0.25 G at 3–200 Hz for 15 min
Storage maximum vibration	0.5 G at 3–200 Hz for 15 min
Operating maximum shock	One shock pulse in the positive z axis (one pulse on each side of the system) of 41 G for up to 2 ms
Storage maximum shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms
Operating altitude	–16 to 3048 m (–50 to 10,000 ft)
Storage altitude	–16 to 10,600 m (–50 to 35,000 ft)

Front view of server

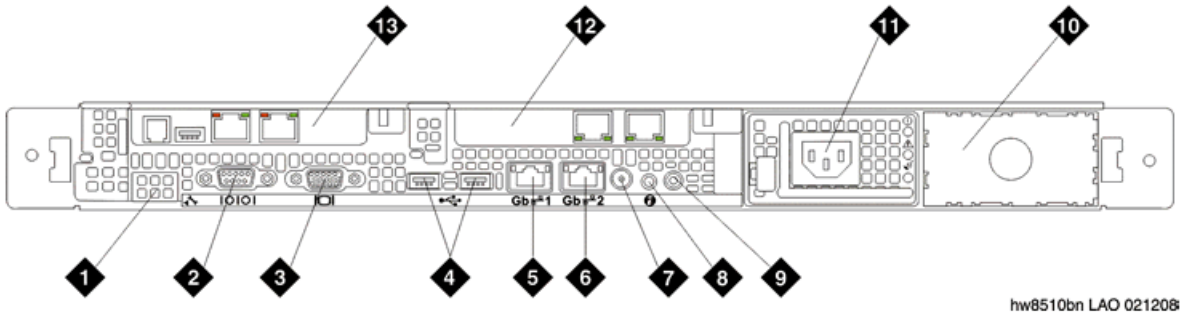


1	Power-on LED
2	NMI button (unused)

3	System ID button
4	LCD display
5	USB ports
6	Video connector (unused)
7	Hard disk drives
8	Optical DVD/CD drive

Back view of server

Note:
For products that do not use the SAMP board, the dual NIC is in the far left slot and the center slot is left empty.



1	Remote access controller (unused)
2	Serial connector
3	Video connector (for optional use of monitor)
4	USB ports (for optional use of modem, mouse and keyboard)
5	GB-1
6	GB-2
7	System status indicator connector
8	System status LED
9	System ID button

10	Bay for optional redundant power supply
11	Power supply
12	Dual NIC
13	Remote maintenance board (SAMP-optional)

Dual Network Interface Card (NIC)

A dual network interface card (NIC) is available and provides two additional Ethernet ports. The dual NIC is optional and comes preinstalled on the server for products that use it.

SAMP overview

The Server Availability Management Processor (SAMP) is a remote maintenance board that monitors and reports alerts from components within the server. The SAMP is optional and comes preinstalled on the server for products that use it.

The SAMP board:

- Monitors the health of the server hardware, including server boot process, the Communication Manager watch dog, the fans, the voltages, and the temperature.
- Reports server failure alarms and other alarms to Avaya INADS or other services group.
  - Server by the server
  - Server by the SAMP, such as server reboots.
  - SAMP by the SAMP

The SAMP presents a virtual TTY that the server uses when the server must send out alarms through the modem. The modem is connected to the USB port on the SAMP board and provides:

- The capability to turn on power and to reset the server remotely.
- A secure dial-in connection to the SAMP and the server.
- Access to the SAMP and subsequently access to the server.

Note:
Modem contention is resolved on a first-come, first-serve basis. For example, Avaya Services dials into the SAMP, and the server must send out an alarm through the modem interface. Although the modem is busy, the server continues to try to send the alarm.

Modem

The modem is used to provide remote access to the server either through the remote maintenance board or direct connection to the server when the customer has a maintenance contract with Avaya. Operating system and environmental alarms are sent through the modem to INADS or other service provider. Maintenance technicians can dial into the server through the modem.

For a server equipped with the Server Availability Management Processor (SAMP) remote maintenance board, the modem connects to the USB port on the SAMP. For a server without the SAMP, the modem connects to a serial port or one of the USB ports on the back of the server.

Important:
The modem must connect to a touch tone line, not a rotary-dial line.

A telephone line connects the modem to a dedicated outside line.

Avaya supports the MultiTech MultiModem ZBA modem for use with the server. This modem provides:

- V.92/56K download speeds and 48K upload speeds when connecting with V.92 servers.
- Linux compatible.
- Globally approved for use in many countries worldwide.
- Flash memory.
- Included USB cable (if a USB modem) or serial cable (if a serial modem).

Compact flash reader

The compact flash memory reader is used to back up files from the server for applications that support it. The reader connects to one of the USB ports and uses a 128-MB Compact Flash card. The compact flash memory reader is optional and comes with the server for products that use it.

Avaya recommends using an industrial grade compact flash card for the following reasons:

- Improved data integrity and reliability with powerful error correction.
- Extreme endurance with 2,000,000 program/erase cycles per block.
- Increased reliability with a mean time between failures (MTBF) greater than 3 million hours.
- 7-year warranty.
- Enhanced durability, using RTV silicone for added strength and stability.

The industrial grade compact flash card is available through Avaya and Avaya business partners.

Related hardware

As part of a total installation, customers may use the following peripheral hardware:

- Uninterruptible power supply (UPS). This can be Avaya or customer provided. If Avaya provided and maintained, then the UPS requires a SNMP module for monitoring. The SNMP module must be configured for traps to be sent.
- Ethernet switch. This can be Avaya or customer provided. If Avaya provided and maintained, then the SNMP agent must be configured for traps to be sent.

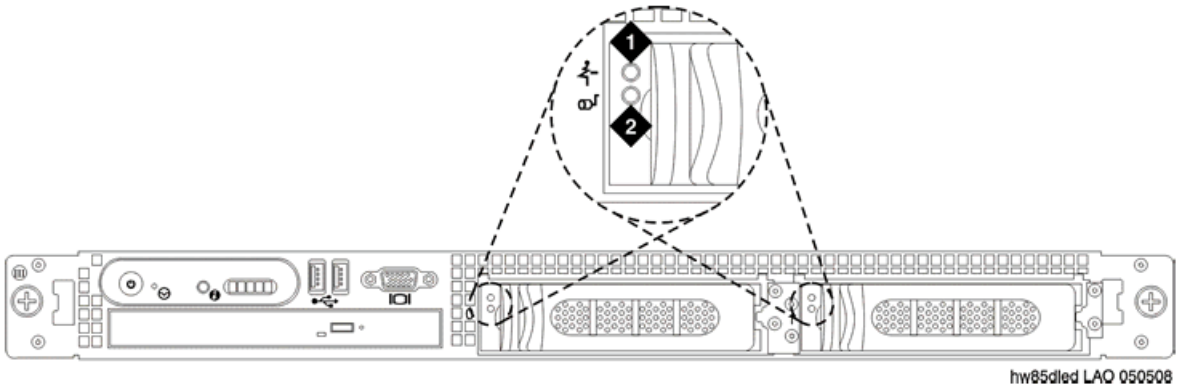
LEDs

The server has two LEDs on the front and 3 LEDs on the back. The dual Network Interface Card has two LEDs per port.

Related topics:

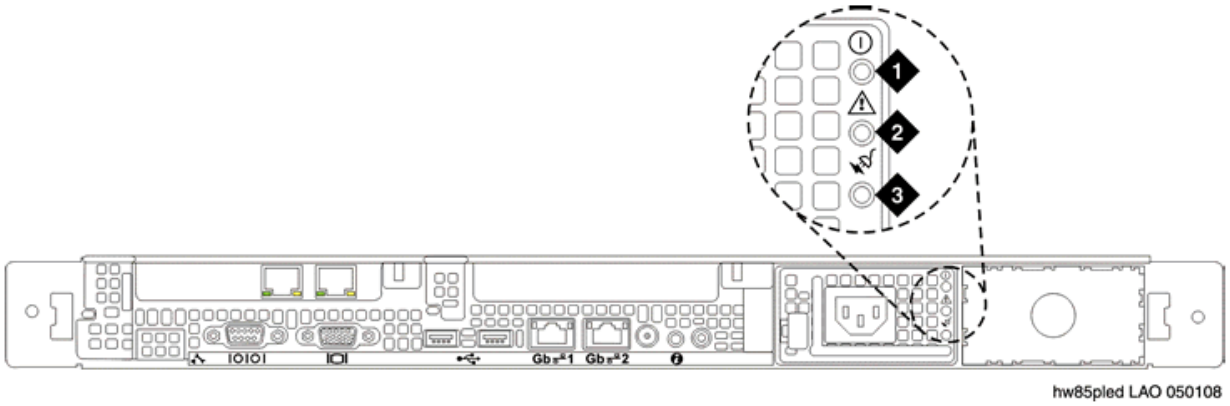
- Front panel LEDs on page 111
- Back panel LEDs on page 112
- LED conditions and patterns on page 112
- Dual NIC LEDs on page 114

Front panel LEDs



1	Drive status
2	Drive activity

Back panel LEDs



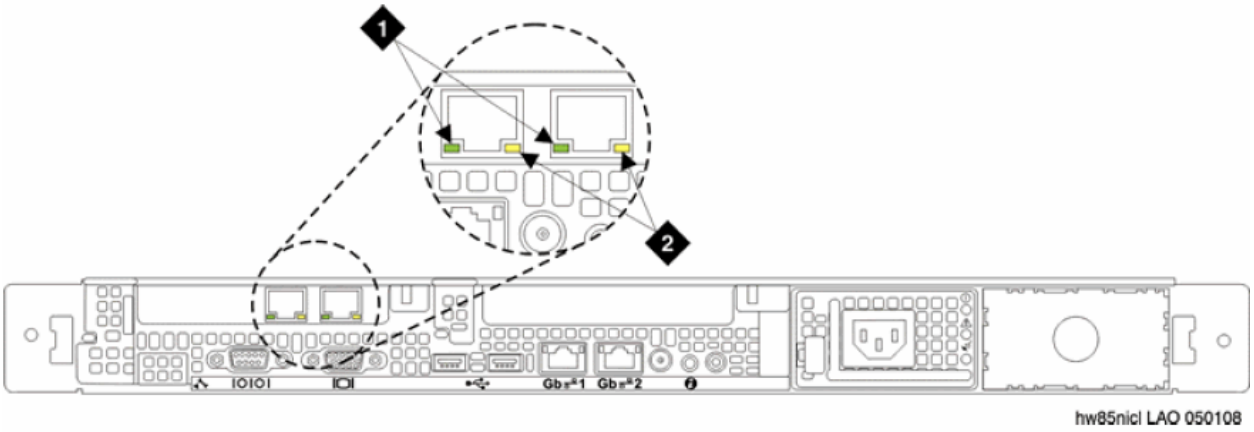
1	Power supply status
2	Power supply fault
	AC line status

LED conditions and patterns

LED	Indicator/Pattern	Function/Condition
Power Status	On	System has power and is opterational
	Off	System has no power
Power supply	Green	Power supply is operational
	Amber	Problem with power supply

LED	Indicator/Pattern	Function/Condition
AC line status	Green	Power supply is connected to a valid AC power source
Drive status	Green steady	Drive online
	Blinks green, then amber, then off	Drive predicted failure
	Amber blinks 4 times per second	Drive failed
	Green blinks 2 times per second	Identify drive/preparing for removal
	Off	Drive ready for insertion or removal
	Green blinks slowly	Drive rebuilding
	Blinks green 3 s slowly, amber 3 s, off 6 s.	Rebuild aborted

Dual NIC LEDs



1	Network activity (TX/RX)
2	Connection rate l Off: 10BaseT active link. l Green: 100BaseT active link. l Amber: 1000BaseT active link.

Server rack installation

Customer-provided equipment

The customer must provide the following equipment:

- Standard 19–in.4–post equipment rack properly installed and solidly secured. Rack must meet the following standards:
  - American National Standards Institute (ANSI) and Electronic Industries Association (EIA) standard ANSI/EIA-310–D-92.
  - International Electrotechnical Commission (IEC) 297.
  - Deutsche Industrie Norm (DIN) 41494.
- Screws that come with the racks for installing the rails.
- USB keyboard, USB mouse, and monitor (optional for some administration).
- AC power from a nonswitched electrical outlet.

- Access to the network.

Avaya-provided equipment

Avaya provides the following equipment:

- Server and power cord
- Static rails rack kit, which contains
  - One pair of static mounting rails with brackets
  - One pair of chassis static rail modules
  - 10–32 x 0.5–in. flange-head cross-head screws (Phillips head)
  - Two, releasable tie wraps.
- Compact flash reader, USB cable, and flashcard (optional for backing up files)
- Modem and USB or serial cable (optional for remote maintenance)
- Other hardware as ordered, such as UPS.

Recommended tools and supplies

You may need the following items to install the server in a 4–post rack:

- #2 crosspoint (Phillips) screwdriver.
- Masking tape or felt-tip pen for marking the mounting holes.

Safety instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system and working environment from potential damage.

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.

CAUTION:
Before installing systems in a rack, install front and side stabilizers on stand-alone racks or the front stabilizer on racks joined to other racks. Failure to install stabilizers accordingly before installing systems in a rack could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizer(s) before installing components in the rack.

After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

Note:
Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements.

System rack kits are intended to be installed in a rack by trained service technicians.

CAUTION:
Always load the rack from the bottom up, and load the heaviest item in the rack first.

Make sure that the rack is level and stable before extending a component from the rack.

Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.

Ensure that proper airflow is provided to components in the rack.

Do not step on or stand on any component when servicing other components in a rack.

Installation checklist

#	Task	Notes	✓
1	Verify that all equipment is on site	Compare the list of items that were ordered to the contents of the boxes. Use the inventory list provided by your project manager; do not rely on the packing slips inside the boxes for the correct information.	
2	Verify that rack is installed to code		
3	Verify that rack is grounded per local code		
4	Remove cabinet doors, if necessary	See cabinet manufacturer's documentation.	
5	Marking the rack on page 118		
6	Attaching rails to the server on page 120		

#	Task	Notes	✓
7	Attaching the rails to the rack on page 121		
8	Installing the server in the rack on page 121		
9	Replace the cabinet doors, if necessary	See cabinet manufacturer's documentation.	
10	Powering up the server on page 122		
11	Troubleshoot the installation		

Marking the rack

Prerequisites

The rack must be installed. If installing the server in a cabinet, then the doors must be removed.

You must allow 1 U (44 mm, or 1.75 in.) of vertical space for each server you install in the rack.

Rack cabinets that meet EIA-310 standards have an alternating pattern of three holes per rack unit with center-to- center hole spacing (beginning at the top hole of a 1-U space) of 15.9 mm, 15.9 mm, and 12.7 mm (0.625 in., 0.625 in., and 0.5 in.) for the front and back vertical rails. Rack cabinets may have round or square holes.

Note:

The vertical rails may be marked by horizontal lines and numbers in 1-U increments. If you want, you can make a note of the number marking on the rack's vertical rail. It is not necessary to mark or place tape on the rack.

CAUTION:

If you are installing more than one server, install the mounting rails so that the first server is installed in the lowest available position in the rack. If you are installing a UPS in the same rack as the server(s), install the UPS in the lowest available position in the rack and the servers above it.

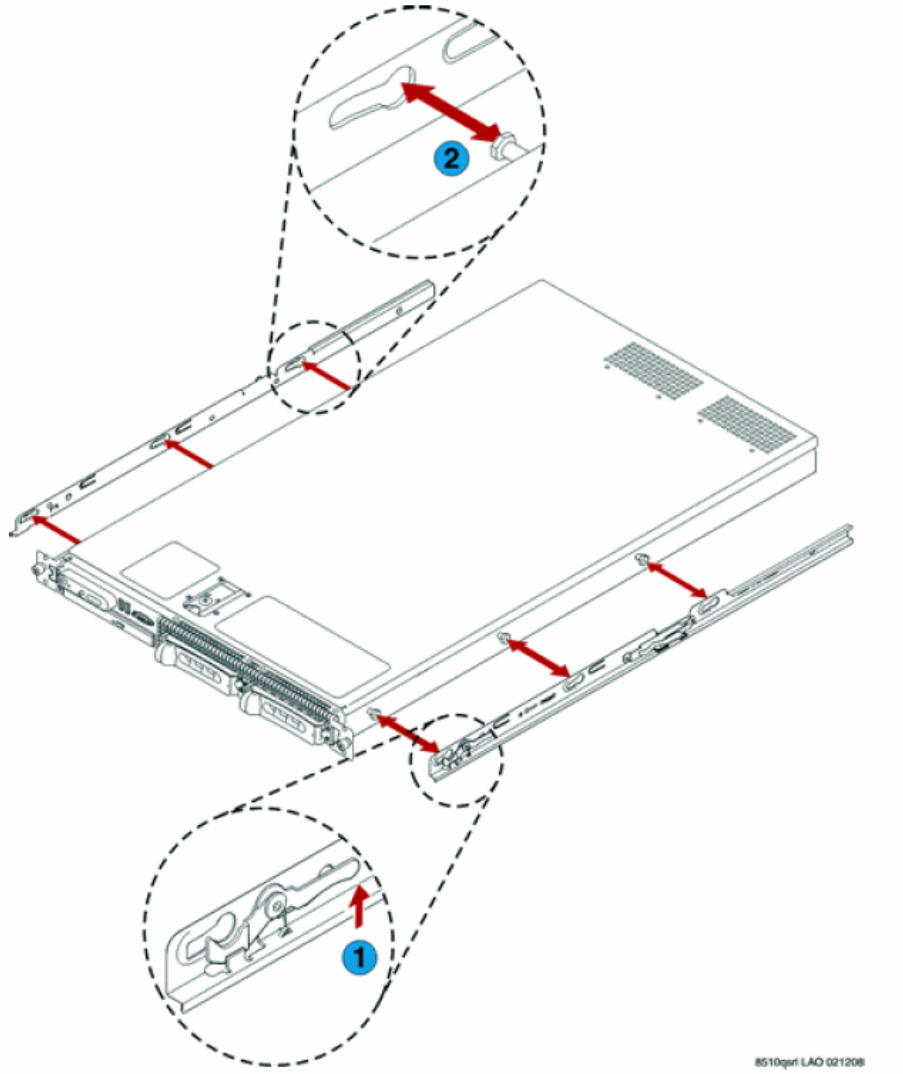
1. Place a mark (or tape) on the rack's front vertical rails where you want to locate the bottom of the server.

The bottom of each 1-U space is at the middle of the narrowest metal area between holes (marked with a horizontal line on some rack cabinets).

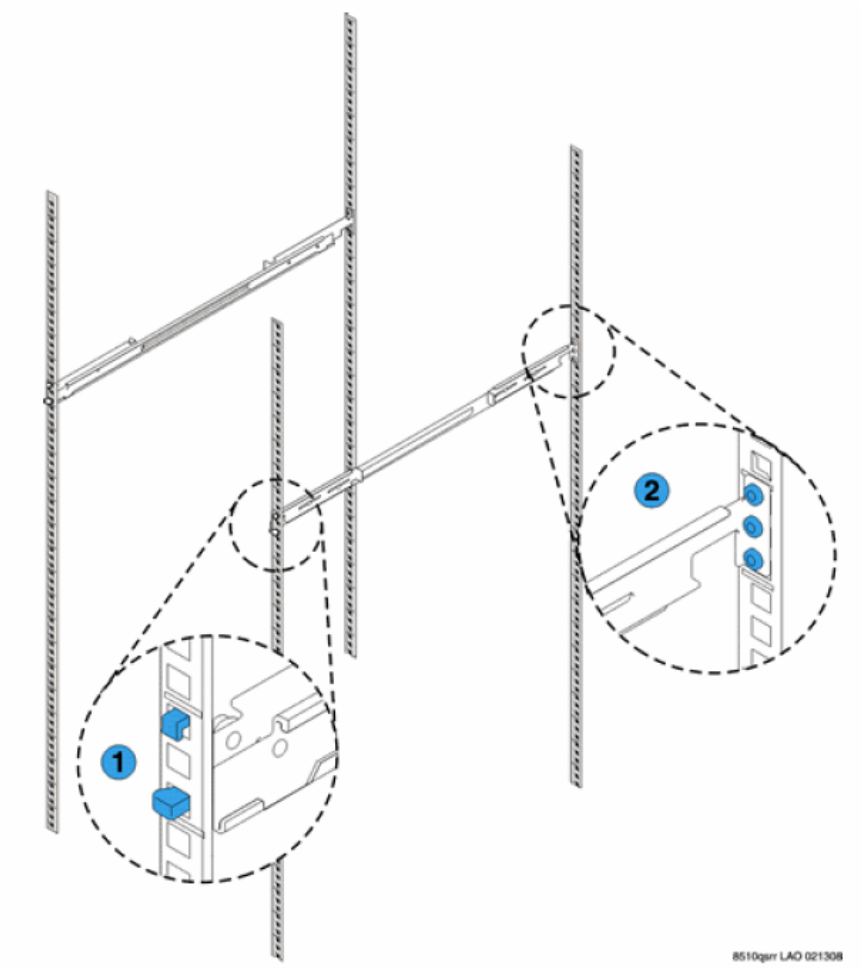
2. Place a mark 1.75 in. (44 mm) above the original mark you made (or count up

three holes in a rack) and mark the rack's front vertical rails with a felt-tipped pen or masking tape. If you counted holes, place a mark just above the top hole. This mark or piece of tape indicates where the system's upper edge will be located on the vertical rails.

Attaching rails to the server



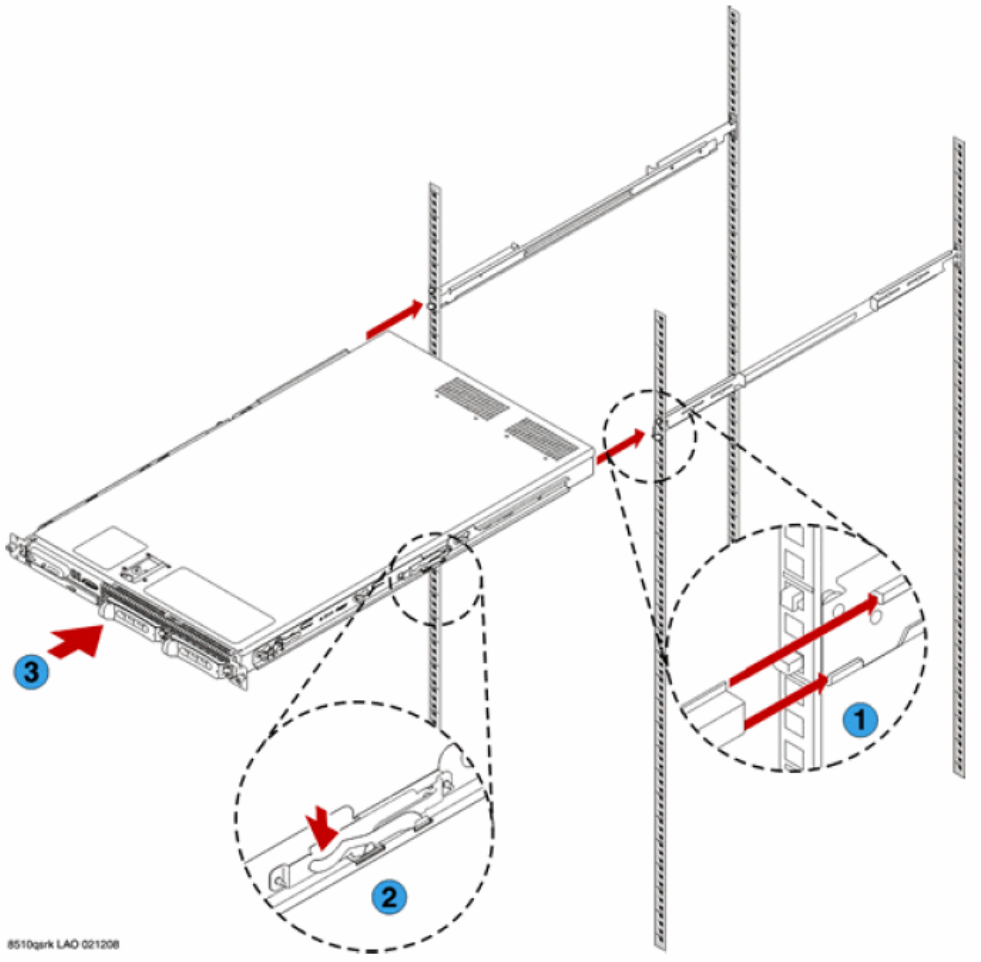
Attaching the rails to the rack



Installing the server in the rack

Prerequisites

The rails must be attached to the server and the rack before installing the server in the rack. If the server is being installed in a cabinet, remove the doors, following the cabinet manufacturer's instructions.



Next steps

If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Powering up the server

Once the server is installed in the rack, you want to power it up to make sure it is working. Once determined, power it down again before inserting any software CD/DVD into the CD/DVD drive.

1. Plug one end of the power cord into the back of the power supply and the other end into a UPS or nonswitched outlet.

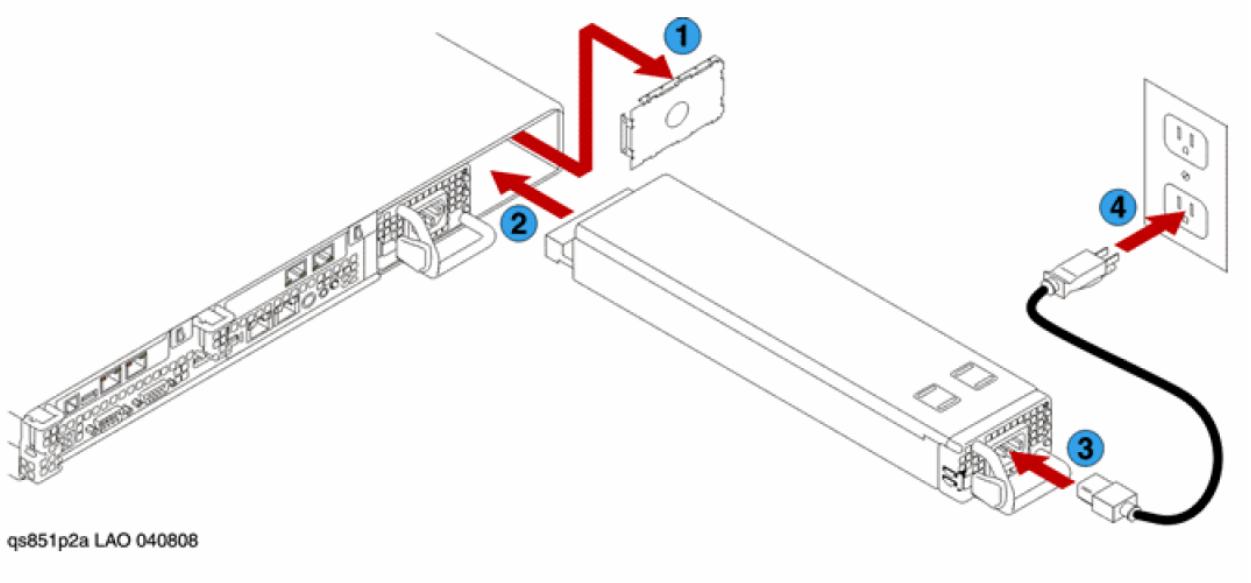
2. Press the power button on the front of the server.
   The green power button lights and the LCD displays Avaya when the power is on.

Next steps

Refer to specific product documentation for information on installing the operating system and software.

Adding a second power supply

You can add a second power supply without powering down the server first.



Next steps

Make sure that the top power supply LED shows green, indicating that it is working.

Troubleshooting the hardware installation

Avaya customer equipment is missing

Proposed solution:

Contact the Avaya project manager

The server has no power

Proposed solution:

- Make sure the power cord is plugged into the back of the server and into a nonswitched outlet or UPS.
- Make sure the UPS is plugged into a nonswitched outlet.
- Make sure the outlet has power.
- Push the power button on the front of the server.

LCD Status messages

The server's control panel LCD provides status messages to signify when the server is operating correctly or when the server needs attention.

The LCD lights blue to indicate a normal operating condition and lights amber to indicate an error condition. The LCD scrolls a message that includes a status code followed by descriptive text. The LCD messages refer to events recorded in the system event log (SEL).

CAUTION:
Only trained service technicians are authorized to remove the server cover and access any of the components inside the system. To prevent damage from static electricity, wear an EMC wrist strap when working inside the server and handling components.

LCD status message explanations

The following table provides the list of codes, the text that goes with the code, the likely causes for the error code, and the corrective action. When escalation is the corrective action, contact Avaya if you have a maintenance contract with Avaya or contact the Avaya business partner from whom you purchased the server. If the escalation requires replacing a field replaceable unit (FRU), see Job Aids for Field Replacements (FRUs) for the Avaya S8510 Server Family (03-602953) for detailed information.

Code	Text	Causes	Corrective Action
N/A	AVAYA	AVAYA displays when: l The system is powered on. l The power is off and active POST errors are displayed.	This message is for information only.
E1000	FAILSAFE, Call Support		Escalate for possible server replacement.
E1114	Temp Ambient	Ambient system temperature is out of acceptable range.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1116	Temp Memory	Memory has exceeded acceptable temperature and has been disabled to prevent damage to the components.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E12nn	xx PwrGd	Specified voltage regulator has failed.	Escalate for possible server replacement.
E1210	CMOS Batt	CMOS battery is missing, or the voltage is out of acceptable range.	Shut down server for 1 hour and disconnect the power supply. If problem continues, escalate for possible server replacement.

Code	Text	Causes	Corrective Action
E1211	ROMB Batt	RAID battery is either missing, bad, or unable to recharge due to thermal issues.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1229	CPU # VCORE	Processor # VCORE voltage regulator has failed.	Escalate for possible server replacement.
E1310	RPM Fan ##	RPM of specified cooling fan is out of acceptable operating range.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1311	RPM Fan Mod #x	RPM of fan x in the # module is out of acceptable operating range.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1410	CPU # IERR	Specified microprocessor is reporting an internal error.	Escalate for possible server replacement.

Code	Text	Causes	Corrective Action
E1414	CPU # Thermtrip	Specified microprocessor is out of acceptable temperature range and has halted operation.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement. **Note**:The LCD continues to display this message until the system's power cord is disconnected and reconnected to the AC power source.
E1418	CPU # Presence	Specified processor is missing or bad, and the system is in an unsupported configuration.	Escalate for possible server replacement.
E141C	CPU Mismatch	Processors are in an unsupported configuration.	Run server diagnostics. This requires a keyboard and monitor.
E141F	CPU Protocol	The system BIOS has reported a processor protocol error.	Escalate for possible server replacement.
E1420	CPU Bus PERR	The system BIOS has reported a processor bus parity error.	Escalate for possible server replacement.
E1421	CPU Init	The system BIOS has reported a processor initialization error.	Escalate for possible server replacement.
E1422	CPU Machine Chk	The system BIOS has reported a machine check error.	Escalate for possible server replacement.

Code	Text	Causes	Corrective Action
E1610	PS # Missing	No power is available from the specified power supply; specified power supply is improperly installed or faulty.	Escalate for possible power supply replacement.
E1614	PS # Status	No power is available from the specified power supply; specified power supply is improperly installed or faulty.	Escalate for possible power supply replacement.
E1618	PS # Predictive	Power supply voltage is out of acceptable range; specified power supply is improperly installed or faulty.	Escalate for possible power supply replacement.
E161C	PS # Input Lost	Power source for specified power supply is unavailable, or out of acceptable range.	Check the AC power source for the specified power supply. Escalate for possible power supply replacement.
E1620	PS # Input Range	Power source for specified power supply is unavailable, or out of acceptable range.	Escalate for possible power supply replacement.
E1624	PS Redundancy	The power supply subsystem is no longer redundant. If the last supply fails, the system will go down.	Escalate for possible power supply replacement.
E1710	I/O Channel Chk	The system BIOS has reported an I/O channel check.	Escalate for possible server replacement.

Code	Text	Causes	Corrective Action
E1711	PCI PERR B## D## F##	Reported a PCI parity error on a component that resides in PCI configuration space at bus ##, device ##, function ##.	Escalate for possible server replacement.
	PCI PERR Slot #	The system BIOS has reported a PCI parity error on a component that resides in the specified PCI slot.	
E1712	PCI SERR B## D## F##	The system BIOS has reported a PCI system error on a component that resides in PCI configuration space at bus ##, device ##, function ##.	Escalate for possible server replacement.
	PCI SERR Slot #	The system BIOS has reported a PCI system error on a component that resides in the specified slot.	
E1714	Unknown Err	The system BIOS has determined that there has been an error in the system, but is unable to determine its origin.	Escalate for possible server replacement.

Code	Text	Causes	Corrective Action
E171F	PCIE Fatal Err B## D## F##	The system BIOS has reported a PCIe fatal error on a component that resides in PCI configuration space at bus ##, device ##, function ##.	Reseat all PCIe cards, then reboot the system. If the problem persists, escalate for possible server replacement.
	PCIE Fatal Err Slot #	The system BIOS has reported a PCIe fatal error on a component that resides in the specified slot.	
E1810	HDD ## Fault	The SAS subsystem has determined that hard drive ## has experienced a fault.	Remove the front bezel and check the top LED on the hard drives. If LED is off or flashing green, then amber, then off or flashing amber 4 times per second, the hard drive is probably failing. Escalate for possible hard drive replacement.
E1811	HDD ## Rbld= Abrt	The specified hard drive has experienced a rebuild abort.	
E1812	HDD ## Removed	The specified hard drive has been removed from the system.	Information only.
E1913	CPU & Firmware Mismatch	The BMC firmware does not support the CPU.	Escalate for possible server replacement.
E1A14	SAS Cable A	SAS cable A is missing or bad.	Escalate for possible server replacement.
E1A15	SAS Cable B	SAS cable B is missing or bad.	Escalate for possible server replacement.
E1A17	Pwr Cable FB	Flex bay power cable is missing or bad.	Escalate for possible server replacement.
E1A18	PDB Ctrl Cable	Flex bay control signals cable is missing or bad.	Escalate for possible server replacement.

Code	Text	Causes	Corrective Action
E2010	No Memory	No memory is installed in the system.	Escalate for possible memory or server replacement.
E2011	Mem Config Err	Memory detected, but is not configurable. Error detected during memory configuration.	Escalate for possible server replacement.
E2012	Unusable Memory	Memory is configured, but not usable. Memory subsystem failure.	Escalate for possible memory or server replacement.
E2013	Shadow BIOS Fail	The system BIOS failed to copy its flash image into memory.	Escalate for possible memory or server replacement.

Removing LCD status messages

For faults associated with sensors, such as temperature, voltage, fans, and so on, the LCD message is automatically removed when that sensor returns to a normal state. For example, if temperature for a component goes out of range, the LCD displays the fault; when the temperature returns to the acceptable range, the message is removed from the LCD. For other faults, you must take action to remove the message from the display.

Power cycle the server.

1. Turn off the system and disconnect it from the electrical outlet.
2. Wait about 10 seconds before reconnecting the power cable.
3. Restart the system.

Using this process, you will not lose the event history for the system.

These actions remove fault messages and return the status indicators and LCD colors to the normal state. Messages reappear under the following conditions:

- The sensor returns to a normal state but fails again, resulting in a new SEL entry.
- The system is reset and new error events are detected.
- A failure is recorded from another source that maps to the same display entry.

Chapter 10: Configuring Communication Manager on the S8510 Server

S8510 port connections

Use standard CAT5 cables with RJ45 connectors on each end to connect to the various ports. If the S8510 Server has only one port network, connect that port network through the dual NIC. S8510 Server connectivity guide shows typical connectivity for the S8510 Server.

Figure 21: S8510 Server connectivity guide

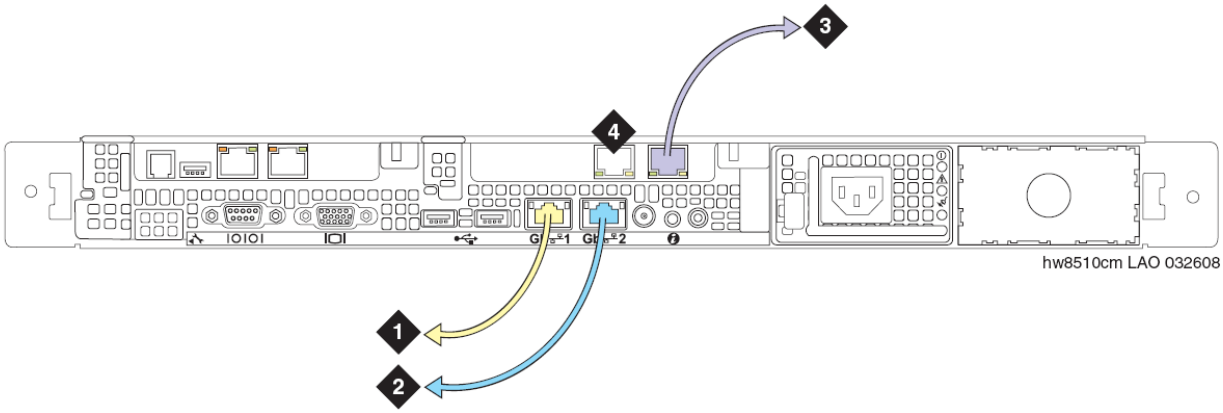


Figure notes:

1. Eth0—To the customer network if the control network is nondedicated. Or, to the control-network Ethernet switch if the control network is dedicated (straight-through CAT5 cable)
2. Eth1—To the Services laptop computer (crossover CAT5 cable)
3. Eth3—to the customer network if the control network is dedicated (straight-through CAT5 cable)
4. Eth4—Not used

S8510 BIOS Upgrade Feature

The **BIOS Upgrade** feature is accessed from the System Management Interface under Server Upgrades.

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:

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

Steps to access a server include:

- Connecting to the server directly on page 137
- Connecting to the server remotely over the network on page 140
- Connecting to the server remotely over a modem on page 140
- Logins for Avaya technicians and Business Partners on page 142
- Configuring the network for Windows 2000 and XP on page 143

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.

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 though 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 Services laptop computer connected directly to the S8500 Server on page 138. Plug the other end of the CAT5 cross-over cable into the NIC on your computer. Use a NIC adapter if necessary.
2. 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 143.

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

Figure 22: Services laptop computer connected directly to the S8500 Server

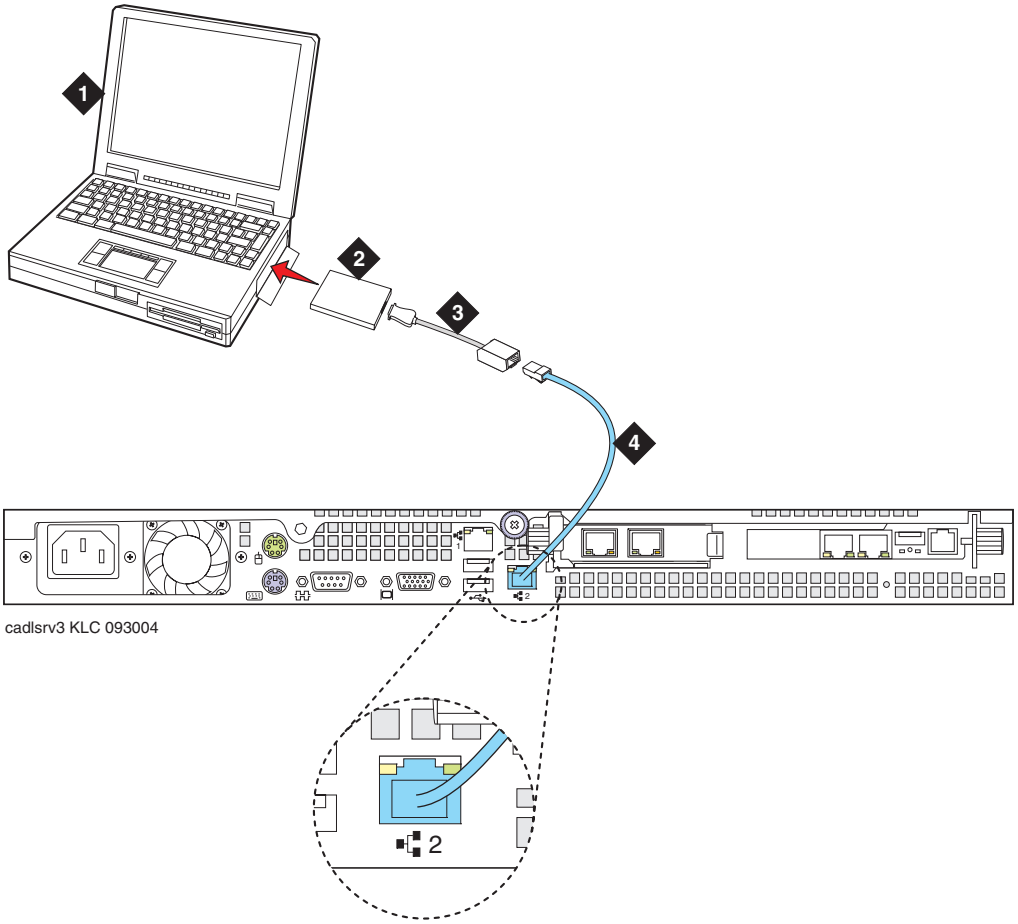


Figure notes:

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

Note:

The layout of the hardware components on the back panel of the S8500C is different from the layout on the S8500B. However, the laptop computer connects to the port labeled `2` on the back panel in both cases. This port is referred to as `Eth1` when configuring the server.

Note:

The layout of the hardware components on the back panel of the S8500C is different from the layout on the S8500B. However, the laptop computer connects to the port labeled `2` on the back panel in the both cases. This port is referred to as `Eth1` when configuring the server.

Figure 23: Services laptop computer connected directly to the S8500 Server

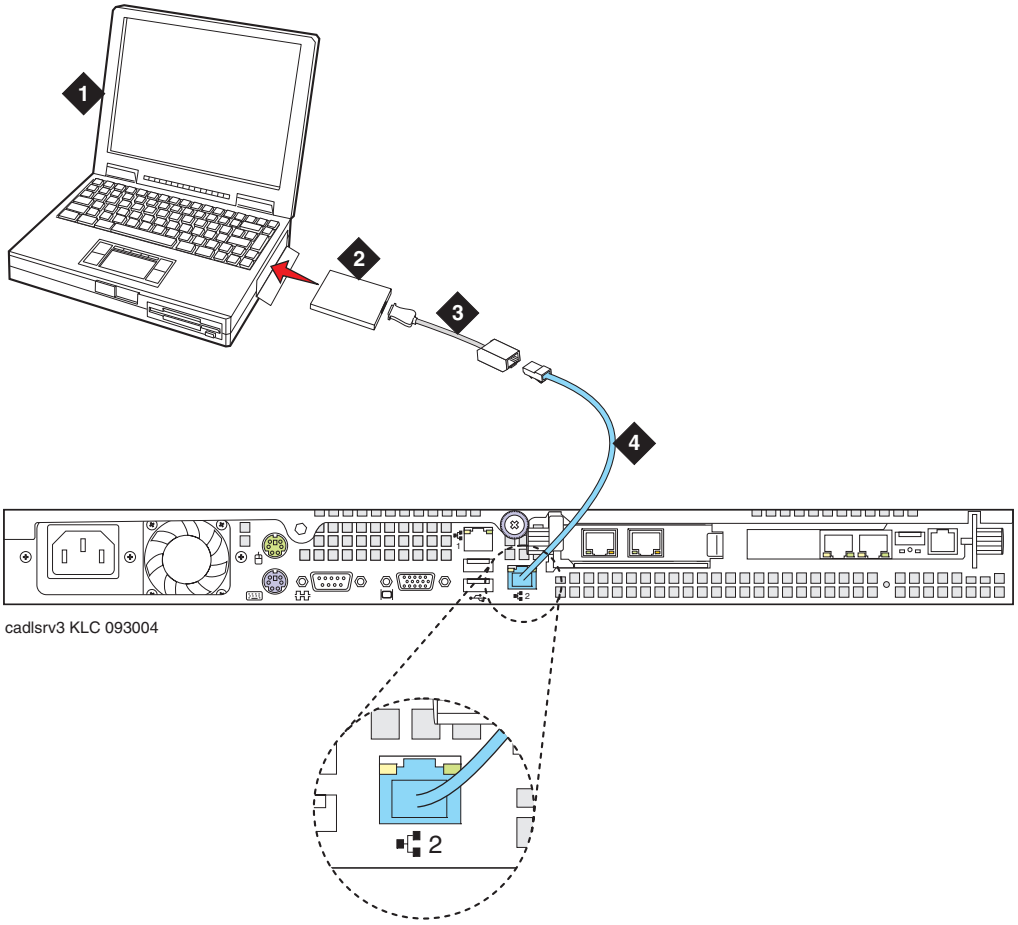


Figure notes:

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

Note:

The layout of the hardware components on the back panel of the S8500C is different from the layout on the S8500B. However, the laptop computer connects to the port labeled `2` on the back panel in both cases. This port is referred to as `Eth1` when configuring the server.

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.

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.

On the S8500 Server, access the server through the remote maintenance board (SAMP) that is installed in the server. For how to access the SAMP, see *Using the Avaya Server Availability Management Processor (SAMP)* (03-300322).

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:
   - Assign a name to the connection.
   - Select dial-up to the network for the network connection type.
   - Select the modem you will be using for the dial-up connection.
   - Enter the appropriate telephone number to access the active server. For the customer-supplied telephone numbers, see the completed *Electronic Preinstallation Worksheet*.
   - 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 135 for more information.
8. Within the SSH client, type the IP address of the active server.

Accessing the System Management Interface

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

- Over the customer network with MS Internet Explorer 6.0 or 7.0.
- Directly to the Services port on the server. For more information, see Services laptop computer connected directly to the S8500 Server on page 138.

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.
6. Open the MS Internet Explorer Web browser to access the System Management Interface.
   - If you are connected directly, in the **Address** field, type `192.11.13.6`.
   - 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 135.
Using SAT with Terminal Emulation	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: • Speed: 115200 baud or 9600 baud if you use a serial modem connection • No parity • 8 data bits • 1 stop bit • No flow control NOTE: Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are the only terminal emulation programs that Avaya supports. Use either the IP address or the DNS host name to establish a network connection to the server. Use port **5023** for this connection. When prompted, log in.

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 145
- Troubleshooting the configuration of the server hardware on page 146
- Troubleshooting the installation of the license file and the Avaya authentication file on page 148

Troubleshooting the installation of the server hardware

Problem	Possible solution
No power to the UPS	• 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	• 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	• 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 IPSI LEDs flash	• 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	l Ensure that the SNMP subagent is installed in the UPS. l Ensure that you are connected to the correct Ethernet port. l Ensure that you have the correct login ID and password. For more information, see the user guide for the SNMP subagent. l Ensure that the network card on the laptop computer is configured correctly.
Cannot log in to the Ethernet switch	l Ensure that you are connected to the correct Ethernet port. (On the Ethernet switch, the correct port is labeled Console) l Ensure that you have the correct login ID and password. See the user guide for the Ethernet switch. l Ensure that the network card on the Services laptop computer is configured correctly.
Cannot log in to the server	l Check the link LED on the server. If the LED is off, a cable or hardware problem exists. l Ensure that you are using SSH and not telnet. l Ensure that you are connected to the Services Ethernet port. l Ensure that you are using a cross-over cable between the Services laptop computer and the server. l 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**. l Ensure that you have connectivity. In an MS-DOS window, type **`ping 192.11.13.6`** and press **Enter**. l Ensure that the NIC on the Services laptop computer is configured correctly.
Cannot access the Avaya Installation Wizard	l Ensure that you are plugged into the Services port. l Ensure that you are using SSH and not telnet. l Ensure that you are using the correct IP address, 192.11.13.6 l Ensure that you are using the correct login and password. l 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	l Ensure that you are using the correct IP address, 192.11.13.6 and port 5023. l Ensure that you are using SSH and not telnet. l Ensure that you are using the correct login and password.
Cannot ping out to the customer network	l Ensure that in the LAN security settings “output from server” for icmp is enabled.
Cannot ping the server from the customer network	l Ensure that in the LAN security settings “input to server” for icmp is enabled.
Cannot access the server remotely	l 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	l The IPSI LED is not programmed with the switch and the location (DHCP) l An IP address is not assigned to the IPSI LED (static IP addressing).
Cannot access the IPSI for static addressing	l Ensure that you are plugged into the Services (top) port on the IPSI. l 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	l 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. l 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	l An IP address is not assigned to the IPSI. l The IPSI is not administered.
The system generates an alarm when first connect to IPSI	l 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	l Provide the correct SAP number. l Provide the serial number for the reference IPSI.
Cannot install the license file	l Ensure that two license files do not exist on the server. If so, delete one of the files. l The file might be corrupt. Download the file again from the RFA site. l Use binary mode to upload the file.
The server is in no-license mode	l 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. l 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	l 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	l Re-install the Avaya authentication files.
Cannot install the authentication file	l Administer a super-user login on the active server.

Index

A

access server
directly . . . 137
remotely over modem . . . 140
remotely over network . . . 140
accessing . . . 141
accessing System Management Interface . . . 141
accessing the server . . . 42
add
IP interface information . . . 72
media gateways . . . 70
administer
IPSI circuit pack . . . 61
AIW. See Avaya Installation Wizard
alarm activation level
setting . . . 72
alarms
enabling to INADS via SNMP . . . 90
setting selected traps . . . 36
to INADS by way of modem, enabling . . . 89
viewing . . . 87
ARP cache, clearing . . . 41
Avaya Installation Wizard, using . . . 48, 52

B

backing up files to compact flash . . . 90

C

C363T or C364T Ethernet switch
configuring . . . 36
LEDs . . . 98
security alert . . . 36
clearing ARP cache . . . 41
command line interface . . . 142
Communication Manager
installing software . . . 41
compact flash, backing up to . . . 90
configure
Avaya C363T or C364T Ethernet switch . . . 36
modem . . . 55
network interface card (NIC) . . . 58
server . . . 45, 69
UPS . . . 33
connect to customer network . . . 25
connection to LAN, verifying . . . 54
copy files to server . . . 47
customer network, connecting to . . . 25

D

date and time, verifying . . . 86
daylight savings rules
location . . . 85
setting . . . 84
DHCP IP addressing
IPSI circuit pack . . . 61
using . . . 66
diffserv parameters, setting . . . 65
direct access to server . . . 137
disable unused Ethernet switch ports . . . 87
disconnecting from server . . . 60

E

EMMC, installing . . . 41, 44
enable Ethernet switch ports . . . 87
environmental specifications
S8500 . . . 21
Ethernet interface assignments . . . 51
Ethernet switch
configuring . . . 38
default IP addresses . . . 37
disabling unused ports . . . 87
preparing to configure . . . 37

F

faceplate
TN2312BP circuit pack . . . 100
firewall settings . . . 55

I

INADS
enabling alarms to by way of modem . . . 89
inputting translations . . . 69
installation
troubleshooting . . . 145
using the Wizard . . . 48, 52
installing
Communication Manager software . . . 43
translation file . . . 73

IP address
set static 62
use DHCP 66
IP address, set static 62
IP interface
enabling control 74
upgrading firmware version 73
verify translations 73
IP interface information
adding to translations 72
IPSI
connecting to 61
LEDs 100
program switch ID and cabinet 61

L

LED
additional information 97
LEDs
Avaya Ethernet switches 98
IPSI 100
S8500 Server 94
UPS 99
license file, testing 93
license server, enabling on a media gateway 79
license, verifying status 74
location
setting for media gateways 85
login, super-user 46
LSP
administer primary controller 78
configuring S8500 as 77
installing the license 79
readminister media gateway controller list 81
resetting 81
S8500 30
S8500, opening TCP ports 80
S8500, verifying primary controller identifies . . . 81
S8500, verifying translations 81

M

manual configuration
configuration, manual method 48
media gateway
enabling license server on 79
media gateways, adding 70
modem
access to server 140
configuring 55
connect to server 27
modem options, setting 28
modem, enabling alarms to INADS 89

N

network interface card (NIC)
configuring 58
network time server (NTP), enabling 56

P

post installation tasks 91
power
applying to server 42
pre-installation tasks at the installation site 15
Processor Ethernet 28, 30

R

remote access to server
over modem 140
over network 140

S

S8500
control network components specifications 19
environmental specifications 21
features and specifications 19
LEDs 94
LSP mode 30
LSP, opening the TCP ports 80
LSP, verifying translations 81
port connections 25
saving translations 69, 73
server
accessing 42
applying power 42
configuring 45, 69
copying files to 47
disconnecting from 60
LED, additional information 97
LEDs 94
verify connectivity 73
verifying LAN connection 54
server configuration, manual method 48
set
alarm activation level 72
daylight savings rules 84
selected traps (alarming) 36
static IP address 62
set static IP address 62
SNMP
preparing to configure 34
SNMP modules
administering 35
software, installing Communication Manager 43

spanning tree
enabling . . . 38
setting version . . . 38
specifications
S8500 . . . 19
S8500 control network components . . . 19
SSH
about . . . 31
static IP addressing
IPSI circuit pack . . . 61
setting . . . 62
static IP addressing, setting . . . 62
super-user login . . . 46

T

table 9 . . . 95
TCP ports, opening on an S8500 LSP . . . 80
Telnet
configuring for Win2000/XP . . . 42
terminal emulation . . . 142
testing
license file . . . 93
server installation . . . 93
TN2312BP . . . 93
TN2312BP
faceplate . . . 100
LEDs . . . 100
program switch ID and cabinet . . . 61
TN2312BP, testing . . . 93
translation file
installing . . . 73
translations
inputting . . . 69
IP interface . . . 69
saving . . . 69, 73
verifying . . . 83
troubleshooting, server installation . . . 145

U

upgrading
IP interface firmware version . . . 73
UPS
default IP addresses for S8400 and S8500 . . . 34
LEDs . . . 99
security alert . . . 33
SNMP module . . . 33
UPS, configuring . . . 33
using DHCP IP address . . . 66
using this documentation . . . 14

V

verify
connectivity to servers . . . 73
date and time . . . 86
IP interface translated . . . 73
license status . . . 74
server connection to LAN . . . 54
translations . . . 83
view alarms . . . 87
VLAN parameters, setting . . . 65

W

Wizard, installation . . . 48, 52