Installing and Configuring the Avaya S8500 Media Server

Release 3.0

03-300143
Issue 3.1
June 2005

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.

Standards Compliance

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.

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997, EN55022:1998, and AS/NZS 3548.

Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

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.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

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

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. 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.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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 G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

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.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
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-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) 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. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

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

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

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. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier’s Declaration of Conformity (SDoC)

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://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

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 (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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://www.avaya.com/support.

Japan

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。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

About this Documentation

This documentation, *Installing and Configuring the Avaya S8500 Media Server* (03-300143) provides procedures for installing Avaya Communication Manager and configuring an S8500 Media Server and other control network components.

Audience

This documentation is for the following people tasked with installing and configuring the media server components:

- Trained field installation and maintenance personnel
- Technical support personnel
- Authorized Business Partners

Using this documentation

Use this documentation as a guide to install and configure the S8500 Media Server. For information about a particular task, use the index or table of contents to locate the page number where the information is described.

For an overview of the installation process, see High level overview of installation process on page 28.

Read Pre-installation information on page 15 first. This section lists all tasks that must be completed before beginning the procedures described in this document. One step you normally complete before going to the customer site is getting the license and Avaya authentication files from the Remote Feature Activation (RFA) Web site.

For technical specifications on the hardware, see Avaya S8500 Media Server features and specifications on page 19.

For the physical installation and cabling of the hardware, see the *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-701). Use the remaining sections of the document in the sequence they are presented. If certain components are not to be installed, skip the procedures for those components. You install and configure the media server components using information in the following sections:

- Configuring the SNMP modules in the UPS on page 32
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) on page 35
- Configuring the media server on page 44
- Configuring the dual network interface card on page 55
- Translating the IPSIs on page 59

You next install the media gateways, using sections in *Installing the Avaya G650 Media Gateway* (03-300144).

Connect the system to the customer's network using information in Connecting to the IPSIs on page 65.

Complete the installation using information in the following sections:

- Completing the installation administration on page 79
- Testing the media server installation on page 89
- Accessing the media server on page 101

If problems occur during the installation, use Troubleshooting an installation on page 111 to try to resolve them.

Conventions

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

General

We show commands and screens from the newest system and refer to the most current books. You must substitute the appropriate commands for your system and refer to the books that you have available.

Physical dimensions

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

Terminology

We use the following terminology in this documentation:

- *Configuration* is a general term that encompasses all references to an Avaya media server with media gateways running Avaya Communication Manager.
- *Cabinet* refers to a stack of media gateways (such as the G650) that are TDM-cabled together.
- *UUCSS* refers to a circuit pack address in cabinet-carrier-slot order.

Downloading this book and updates from the Web

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

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

Downloading this documentation

To download the latest version of this documentation:

1. Access the Avaya Support Web site at http://support.avaya.com.
2. Type the documentation number in the Search Support box in the upper left and click **Go**.

   The system displays the Product Documentation Search Results page.
3. Or click **Product Documentation**.
4. From the menu on the left, select Communications Systems.
5. Scroll down to find the product and latest release number.

6. Click the release number to view the list of titles.
7. Click on the title that you want.
8. Click one of the following options:
   - **PDF Format** to download the book in regular PDF format.
   - **ZIP Format** to download the book in zipped PDF format.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

CAUTION:
A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

WARNING:
A warning statement calls attention to a situation that can result in harm to hardware or equipment.

Use an ESD warning to call attention to situations that can result in ESD damage to electronic components.

DANGER:
A danger statement calls attention to a situation that can result in harm to personnel.

SECURITY ALERT:
A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

Related resources

For providing physical installation and connection information, see *Quick Start for Hardware Installation: Avaya S8500 Media Server,* 555-245-701.

Additional information on installing some adjunct and peripheral equipment that an S8500 media server supports is contained in *Adding New Hardware—S8500, S8700, and S8710 Media Servers* (555-233-112).

For all documents associated with the S8500 Media Server, including those described above, see *Documentation for Avaya Communication Manager, Media Gateways and Servers* CD (03-300151).

Technical assistance

Avaya provides the following resources for technical assistance.

Within the U.S.

For help with:

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

International

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

Trademarks

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

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.
  Product Documentation Group
  Room B3-H13
  1300 W. 120th Ave.
  Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Make sure that you mention the name and number of this book, *Installing and Configuring the Avaya S8500 Media Server* (03-300143).

Chapter 1: Introduction

These procedures are for installing Avaya Communication Manager and configuring a new Avaya S8500 Media Server and associated components in either an IP Connect or direct connect configuration.

As part of the procedures for configuring the various pieces of hardware, you use two administration interfaces: the Maintenance Web Interface and a command line interface using either telnet or a terminal emulation program such as Avaya Native Configuration Manager. You also use the Avaya Installation Wizard to configure the media server.

There are no requirements to install the media server before the media gateways; however, the license file only allows 30 minutes to "see" the administered and connected IP Server Interface (IPSI) circuit packs.

The following information is included in this installation procedure:

Pre-installation information

There are several tasks that you need to verify before you go on site and before you start the installation. If the pre-installation team did not complete them, do not continue with the installation.

Before you go on site

Before going on site, make sure the customer has power, a local area network set up and running, and a network administrator available the day of the installation. Before beginning the software installation and media server configuration, make sure you have the filled-out *Electronic Preinstallation Worksheet* (EPW) on the services laptop. See the Avaya Installation Wizard Web site (http://support.avaya.com/avayaiw) for the blank form.

If you are staging the installation at a location other than the customer's site, verify that you have all the equipment by comparing the list of items ordered against the items in the boxes. Your project manager can supply you with an inventory list. Do not rely solely on the packing slips inside the boxes.

In addition, the pre-installation team should have done the following tasks. If they were not all done, do not continue with the installation.

- Verify that the services laptop has the right hardware and software. See Connecting to the media server directly on page 101 for the list of computer hardware and software specifications.
- Verify that you have current translations available for download via ProVision.
- Verify that you have a filled-out *Electronic Preinstallation Worksheet* (EPW). The EPW provides
  - IP addresses
  - Product ID (same for both media server and remote maintenance board)
  - Avaya services telephone number for remote access over modem
  - Avaya services IP address for alarms through the network
- Verify that you have the current software update, if required, and license and Avaya authentication files on your services laptop.
- Verify that you have the current firmware available, including for the BIOS. Firmware for the IPSIs, C-LAN, MedPro, and VAL circuit packs are on the software CD, but check the Avaya Support Web site (http://support.avaya.com), Download Software and Firmware, for the latest software and firmware.
- Verify that you have all the login IDs and passwords to access the S8500 Media Server, maintenance adapter, and server complex components. This includes the unique service password for that customer's equipment.

  To obtain the password for a specific media server, call ASG Conversant (1.800.248.1234 or 1.720.444.5557). You must have the IL, FL, or product ID to get the password.

  To log in through the services port as craft after you install the Avaya authentication file, use this password, which does not require an ASG challenge or response.

Downloading license and Avaya authentication files

Use Remote Feature Activation (RFA) to obtain the Communication Manager license and Avaya authentication files. RFA is a Web-based application, available to Avaya employees and authorized BusinessPartners, that enables you to create and deploy license files for all Communication Manager product platforms. The RFA Web site is at http://rfa.avaya.com. For specific information on RFA and how to generate license and Avaya authentication files, go to the the RFA Information page available on the RFA Web site.

Note:

To access the RFA application, you must complete the RFA online training and have received access authorization.

To generate a license file, you need the following information:

- Your personal Single Sign-On (SSO) for the RFA Web site authentication login.
- SAP order number
- Required customer information
- For a new license, the serial number of one TN2312BP Internet Protocol Server Interface (IPSI) circuit pack designated the reference IPSI.
- For an updated license, the RFA system ID (SID) for the existing media server, which is necessary to locate the existing license.
- Internet access to the RFA Web page with Internet Explorer 5.0 or higher.

Before arriving on site, download the license and Avaya authentication files to the services laptop. The license and Avaya authentication files are installed during the installation process.

Once the Avaya authentication files are installed, Avaya services logins to the media server are protected by a challenge/response system called Access Security Gateway (ASG). The ASG challenge/response protocol confirms the validity of each user, reducing the opportunity for unauthorized access.

When finished installing the Avaya authentication file, Avaya Communication Manager has a password for the craft login. This password is unique to the customer's server. You can use the password the next time you log in as craft, provided you access the media server through the services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access still requires an ASG challenge/response. The revised password is recorded by RFA and is obtained from ASG Conversant at 1-800-248-1234 or 1-720-444-5557.

Copying files to the laptop

In addition to the license and Avaya authentication files, you must copy other required files to the services laptop. This includes the filled-out *Electronic Preinstallation Worksheet* (EPW); any software updates; current firmware, including firmware for the BIOS, maintenance adapter, and programmable circuit packs.

To get a filled-out EPW, go to the project manager or customer. To get a blank EPW, go to the Avaya Installation Wizard Web site (http://support.avaya.com/avayaiw). Have the customer fill it out.

To get the software update, go to the Avaya Support Web site (http://avaya.com/support) and select **Software & Firmware Downloads** to identify and copy the required software update.

To get the latest firmware for the BIOS, remote maintenance board, and programmable circuit packs, go to the Avaya Support Web site at http://avaya.com/support and select **Software & Firmware Downloads** to identify and copy the latest firmware.

Before you start the installation

Before beginning the installation, verify that you have all the equipment on site by comparing the list of items ordered against the items in the boxes. Your project manager can supply you with an inventory list. Do not rely solely on the packing slips inside the boxes. For a partial list of required hardware, see List of required hardware on page 21.

The pre-installation team should have done the following tasks. If they were not all done, do not continue with the installation.

- Verify that the open, customer-supplied, EIA-310D (or equivalent) standard 19-in. (48-cm) 4-post equipment rack(s) is(are) properly installed and solidly secured. Make sure that the screws that come with the racks are there. If using a rack cabinet, make sure it has adequate ventilation.
- Verify that the rail kit to support the media server is available for installation.
- Verify that the rail kit, required to support the very heavy UPS, is installed on the rack or available for installation. For information on installing the rails, see the documentation that comes with the rail kit.
- Verify that the equipment rack(s) is(are) grounded per local code. See *Job Aid: Approved Grounds* (555-245-772).
- Verify that the customer provides AC power to the rack from a nonswitched outlet.
- Verify that cabling for the TN2312BP IP Server Interface (IPSI) circuit packs is labeled and run from the control hardware rack to the port networks or that appropriate connectivity is provided.

Equipment specifications

The media server control network components consist of the media server, one UPS, and an Avaya-provided Ethernet switch (optional). See Table 1: Control network components specifications.

Table 1: Control network components specifications

Component	Dimensions English (in.)	Metric (cm)	Us (height)	Weight (lb/ kg)
Media Server: S8500	1.75h x 17w x 20d	4h x 43w x 51d	1	28/13
Ethernet Switch: C363T C364T	 1.75h x 17w x 14.4d 1.75h x 17w x 14.4d	 4h x 43w x 37d 4h x 43w x 37d	 1 1	 11/5 11/5
UPS: 700 VA 1500 VA	 3.5h x 17w x 19d 3.5h x 17w x 24d	 9h x 43w x 48d 9h x 43w x 61d	 2 2	 34/15 50/23

The internal room temperature must not exceed 104° F (40° C).

Table 2: Avaya S8500 Media Server features and specifications outlines the features and specifications of the Avaya S8500 Media Server.

Note:

Some values are shown at maximum configuration. Avaya values will be slightly lower then the maximum.

Table 2: Avaya S8500 Media Server features and specifications

Feature	Specifications
Microprocessor	One Pentium 41024-KB Level-2 cache and MMX (MMX2) technology
Memory	512 MB Type: PC2700/3200 266 MHz, ECC, SDRAM, registered DIMMs only Slots: Four dual inline
Drives	Diskette: 1.44 MB CD/DVD-ROM: IDE
Power Supply	300 watt (110 or 220 VAC auto-sensing)

1 of 2

Table 2: Avaya S8500 Media Server features and specifications (continued)

Feature	Specifications
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 Diskette drive
Acoustical Noise Emissions	Sound power, idling: 6.5 bel maximum Sound power, operating: 6.5 bel maximum
Environment: Air Temperature	Media server on: ● 50.0° to 95.0° F (10° to 35° C) ● altitude: 0 to 2999 feet (0 to 914 meters) Media server off: ● -104° to 140° F (-40° to 60° C) maximum altitude: 6998 feet (2133 meters)
Environment: Humidity	● Server on: 8% to 80% ● Server off: 8% to 80%
Heat Output	Minimum configuration: 297 BTU (87 watts) Maximum configuration: 512 BTU (150 watts)
Electrical Input	Sine-wave input (47-63 Hz) required Input voltage low range: ● Minimum: 100 VAC ● Maximum: 127 VAC Input voltage high range: ● Minimum: 200 VAC ● Maximum: 240 VAC Input kilovolt-amperes (kVA) (approximate): ● Minimum: 0.0870 kVA ● Maximum: 0.150 kVA Receptacle U.S.: XXXX 87=NEMA 5-15 Circuit Breaker: XXXX 87=15 amp Pole: XXXX 87=1 Amp Draw: ● 100-127 V~ 4.6 A ● 200-240 V~ 2.3 A

2 of 2

Required hardware

Before beginning the process, make sure you have the hardware listed in Table 3: List of required hardware and Table 4: List of S8500 Media Server optional localization kits on page 22 on hand.

Table 3: List of required hardware

Comcode	Description	Number	Included	Optional	FRU
700328339	S8500 Media Server w/AC power	1	Yes		Yes
NA	Rail kit for S8500 (IBM 32P9107)	1	Yes		No
408357002 408427409 700181928	Powerware 9125 uninterruptible power supply (UPS) (if Avaya-provided) – US & Canada – International – Japan	1		Yes (can be customer provided)	Yes
408427656	SNMP Network Interface Adapter for UPS (if Avaya-provided)	1		Yes	Yes
700230741	Rail kits for mounting UPSs in rack – 4-post rack (Powerware code: 05146726-5501)	1		Yes	Yes
700319932 700319940	10/100BaseT Ethernet switch (if Avaya-provided) – C363T Avaya Ethernet switch – C364T Avaya Ethernet switch	1		Yes	Yes
700169121	External V.90 56K USB modem with cable (if used)	1	Yes		Yes
700277551	Serial modem (requires one localization kit) (S8500A only)	1	Yes		Yes
700289580	Compact flash disk memory reader	1	Yes		Yes
N/A	Compact flash disk	1		Yes	Yes
700284623	Dual Network Interface Card (NIC)	1	Yes (if only 1 PN)	Yes	Yes
700287964	Avaya Communication Manager CD for Linux Servers		Yes		Yes

1 of 2

Table 3: List of required hardware (continued)

Comcode	Description	Number	Included	Optional	FRU
700349822	Documentation for Avaya Communication Manager, Media Gateways and Servers CD		Yes		Yes
700170012 700178056 700178064	Green CAT5 Ethernet cables – 5-meter (16 feet) – 25-meter (82 feet) – 50-meter (164 feet)	 4 2-68 2-68	Yes		Yes
700170053	Black CAT5 Ethernet crossconnect cable for laptop computer		Yes		Yes
407063478	Electrostatic discharge (ESD) wrist strap	1	Yes		Yes
					2 of 2

Table 4: List of S8500 Media Server optional localization kits

Comcode	Description	Number	Included	Optional	FRU
700277569	Localization kit LK-ZBA-US			Yes	Yes
700277577	Localization kit LK-ZBA-EURO			Yes	Yes
700277593	Localization kit LK-ZBA-AU			Yes	Yes
700277668	Localization kit LK-ZBA-GB/IE			Yes	Yes
700277676	Localization kit LK-ZBA-IN+			Yes	Yes
700277700	Localization kit LK-ZBA-NZ			Yes	Yes

Remote Maintenance Board

The remote maintenance board monitors and reports alerts on the Avaya S8500 Media Server components and provides control to power the media server on and off the. The S8500 Media Server uses the Server Availability Management Processor (SAMP).

Server Availability Management Processor

The Server Availability Management Processor (SAMP) is a remote maintenance board that is pre-installed in the S8500 Media Server and provides remote maintenance and serviceability to the media server.

SAMP functionality

Note:

Only the fields that need to be added or changed for an Avaya installation are outlined in this section.

Modem contention is resolved on a first-come first-serve basis. For instance, if services dials into the SAMP, and the media server needs to send out an alarm through the modem interface, it will find the modem busy, but will continue to try to send the alarm.

The SAMP card provides the following functionality:

- Monitors the media server state of health: fans, voltages, and temperature
- Reports media server failure and other alarms to INADS by modem
- Provides remote media server power-on and reset capability
- Secure dial-in connection to the SAMP and the host
- Services laptop access to the SAMP (and subsequently the host)

The SAMP presents a virtual tty that the media server makes use of when it needs to send out alarms through the modem interface (see Figure 1: SAMP rear connections on page 24). The system uses the modem that is connected to the USB port off of the SAMP card for:

- Reporting alarms on the media server by the media server
- Reporting alarms on the media server by the SAMP, for example, server reboots
- Reporting alarms on the SAMP by the SAMP
- Services dial-in access to the media server and the SAMP for remote maintenance and administration purposes

SAMP connections

The SAMP card is installed in PCI-X slot 1 (full-height, 3/4 length slot) of the Avaya S8500 Media Server.

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

- SAMP Ethernet 1 is not used.
- SAMP Ethernet 2 is for local Services laptop access. This is for on-site services personnel to access the SAMP using the craft login.
- The USB interface is used to connect a USB modem that is used for remote dial-in and dial-out access. This modem connection is shared between the media server and the SAMP for remote maintenance, administration, and alarming purposes. For dial-in purposes, the user first establishes a ppp session that terminates at the SAMP. The user then can establish an SSH (Secure Shell) or HTTPS (Secure Web) session to the SAMP or the host using the craft login.

The SAMP also communicates with the host in-band via an on-board industry standard Ethernet controller on the host's PCI bus with an internal link to the SAMP.

See Figure 1: SAMP rear connections for locations of the connections on the SAMP.

Figure 1: SAMP rear connections

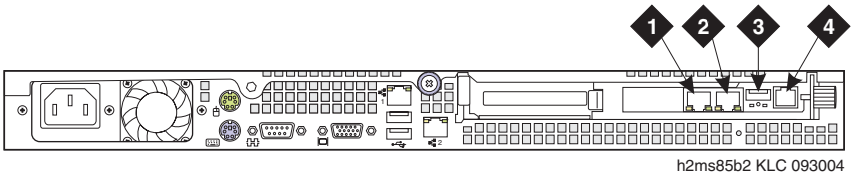


Figure notes:

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

SAMP software

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

If a SAMP software update file is available on the Avaya Support website, you should have downloaded it to your laptop. See *The Avaya Server Availability Management Processor User Guide*, 03-300322, for details on installing software on the SAMP and changing default settings.

Documentation

We recommend that you have the following documents on hand for the installation. These are included on the *Documentation for Avaya Communication Manager, Media Gateways and Servers* CD (03-300151).

- *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-701)—a quick reference guide providing physical installation and connection information.
- Filled-out *Electronic Preinstallation Worksheet*—An Excel spreadsheet providing the customer's network information needed to use the Avaya Installation Wizard to configure the control network components. Get from the Avaya project manager, Avaya software technician, or customer network administrator. A blank one is available at the AIW Web site (http://support.avaya.com/avayaiw).
- *Installing and Configuring the Avaya S8500 Media Server* (03-300143)—this document, providing information on configuring the control network components, testing, and troubleshooting.
- *Avaya Server Availability Management Processor User Guide* (03-300322)—documentation providing information on administering the SAMP.
- *Job Aid: Approved Grounds* (555-245-772)—job aid providing a description of all approved grounds.
- *Upgrading Software and Firmware—Avaya S8500 Media Server* (555-245-111)—part of the library providing information on upgrading Avaya Communication Manager and firmware for various components and circuit packs.
- *Administrator's Guide for the Avaya Communication Manager* (555-233-506)—end-user documentation that includes information on administering trunks and telephones.
- *Administration for Network Connectivity for the Avaya Communication Manager* (555-233-124)—documentation providing information on network connectivity.
- *Maintenance Alarms for Avaya Communication Manager 3.0, Media Gateways and Servers* (03-300430)—provides information on how to troubleshoot and replace various components.
- *Maintenance Commands for Avaya Communication Manager 3.0, Media Gateways and Servers* (03-300431)—provides information on how to use command interfaces, command syntax, and output from maintenance-related commands.
- *Maintenance Procedures for Avaya Communication Manager 3.0, Media Gateways and Servers (*03-300432)—provides information on how to use alarms, error codes, and tests to diagnose and repair problems.

Connecting the Ethernet ports

The following section provides information on connecting the Ethernet ports on the back of the media server.

You connect to the various ports using standard CAT5 cables with RJ45 connectors on each end. If the S8500 Media Server has only one port network, connect it through the dual NIC. Figure 2: Avaya S8500 Media Server connectivity guide shows typical connectivity for the S8500 Media Server.

Figure 2: Avaya S8500 Media Server connectivity guide

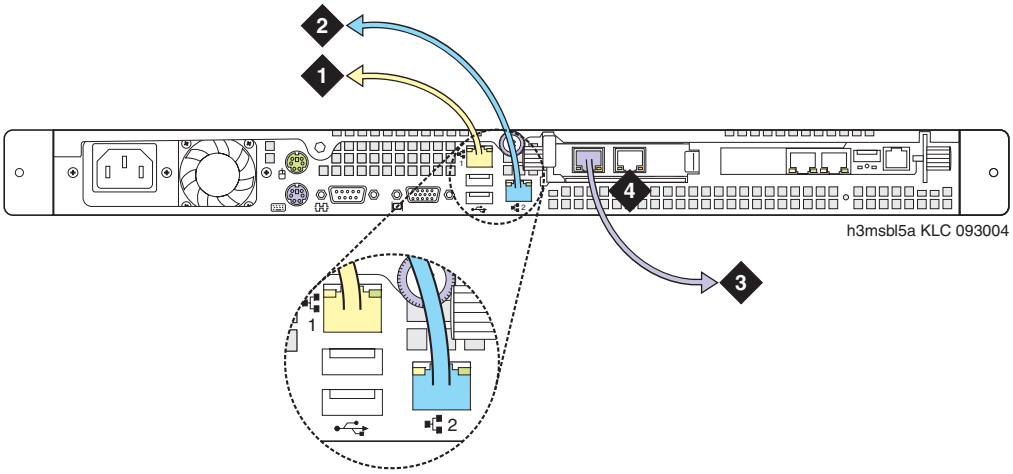


Figure notes:

1. Eth0—to customer's network if nondedicated control network. (straight-through CAT5 cable)
2. Eth1—to services laptop (cross-connect CAT5 cable)
3. Eth2—to port network if only one port network (cross-connect CAT5 cable) *or* to customer's network if dedicated control network (straight-through CAT5 cable)
4. Eth3—unused

Connecting the modems

On an S8500 Media Server, there is a modem that connects to the USB port on the SAMP. If you have not connected the modem yet, do so now.

Note:

USB modems cannot connect to rotary lines. A Touch Tone line is required.

Required options on the SAMP modem are set by Avaya defaults on the SAMP. For a modem connectivity diagram see Figure 3: Modem connectivity on the Avaya S8500 Media Server.

Figure 3: Modem connectivity on the Avaya S8500 Media Server

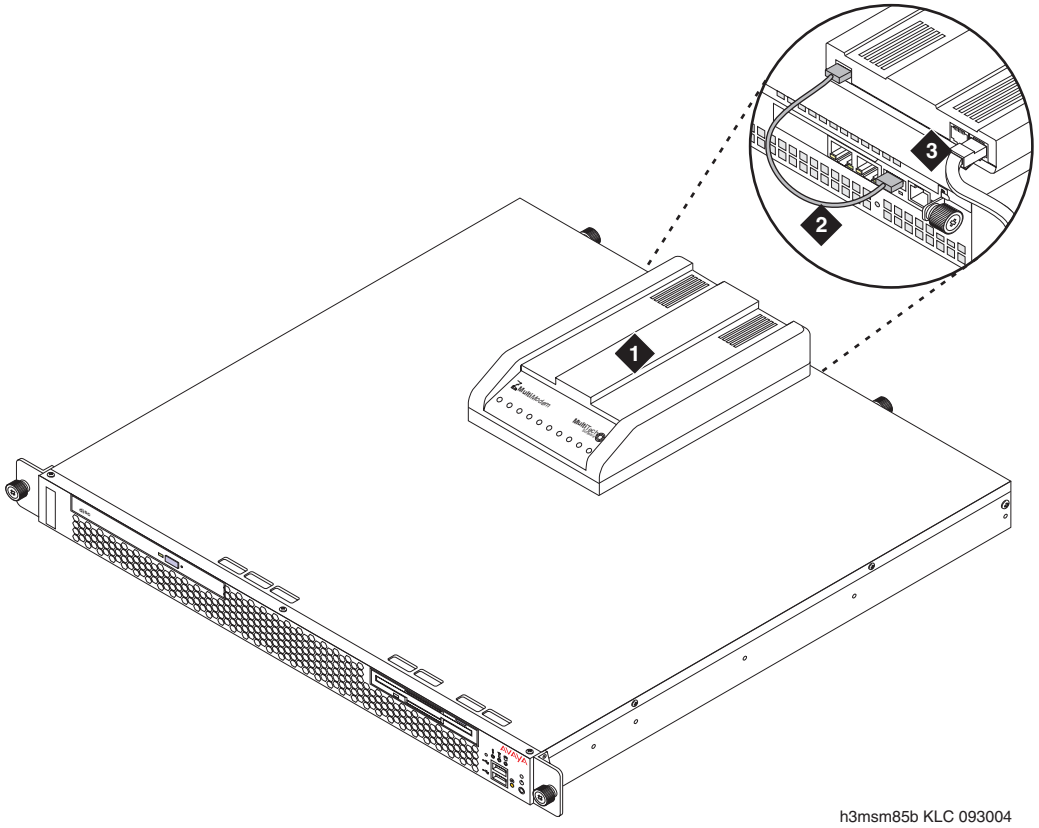


Figure notes:

1. Modem
2. USB cable connecting the USB modem to the USB port on the media server.
3. Telephone line connecting the modem to the outside line.

To connect the modem:

1. Terminate the 1-MB telephone line at the RJ11 jack outlet.
2. Connect the telephone line to the modem with the modular telephone cord supplied with the modem.
3. Connect the USB cable from the USB modem to the USB port on the SAMP.

High level overview of installation process

The installation process is completed in stages. Some stages can be completed in parallel, and others require that certain tasks be accomplished before the stages can be completed. The order that the particular stages are completed depends on local practice and the personnel available. The high level stages are listed below.

Installing and cabling the media server complex

You can complete this stage before, in parallel with, or after installing the media gateways. See the *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-703)

Installing Avaya Communication Manager

The media server is shipped with a blank hard drive. The operating system, directories, and files needed for the media server are installed from a bootable CD containing the operating system and Avaya Communication Manager. This stage is usually done immediately after installing the media server hardware.

Note:

If you are installing an S8500B Media Server to run the Expanded Meet-me Conferencing (EMMC) application, repeat these first two steps for that media server. After you have installed the hardware and Communication Manager software on the EMMC S8500B, use *Expanded Meet-me Conferencing (EMMC) version 1.0 Installation and Troubleshooting Guide*, 04-300527.

Configuring the remote maintenance board

The remote maintenance board, which is the Server Availability Management Processor (SAMP), monitors various components and environmentals on the media server. The board comes installed from the factory with Avaya defaults but must be configured to fit your specific installation. The SAMP is administered automatically through the Avaya Installation Wizard

Configuring the media server

Use the Avaya Installation Wizard to configure the media server. You must have the filled-out *Electronic Preinstallation Worksheet* (EPW) that provides the customer's network information needed for configuring the network components. As part of the Wizard, you install the license and Avaya authentication files. This stage is done after installing the software.

Translating the IPSIs

This stage is done after the media server is configured. Once the license file is installed (as part of the Avaya Installation Wizard), you have 30 minutes to complete this step before the license file looks for the reference IPSI.

Installing and cabling the media gateways

You can do this stage before, in parallel with, or after installing and configuring the media server complex. The media gateways must be installed and powered up to effectively complete many of the other stages. The IPSI circuit packs can only be programmed in a powered up media gateway.

Completing the installation administration

This stage finishes the installation. Clearing alarms, enabling alarm reporting, backing up the server files, and registering the configuration. This stage always comes at the end of the complete installation.

Testing the complete installation

This stage verifies the complete configuration operation and is the last task.

Chapter 2: Configuring the hardware in the rack

Once the control network equipment is installed and connected, you must configure the media server, the SNMP Module in the UPS (if Avaya supplied), and the SNMP Subagent in the Avaya Ethernet switch (if Avaya provided). The SNMP components enable their hosts to send alarms (traps) to the media server.

Configure the SNMP agents first, then install Avaya Communication Manager on and configure the media server and verify its operation.

This section covers the following procedures:

Configuring the SNMP modules in the UPS

Note:

These instruction apply only if using 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 non-Avaya-provided UPS.

Note:

Because the SNMP module is manufactured by a third party, we do not know which brand, model, or firmware load the factory is shipping. Therefore, we cannot provide specific instructions in this document on how to connect to and configure the SNMP module. Refer to the documentation that comes with the SNMP module.

Note:

If the control network is non-dedicated (going over the customer's network), you must make sure that the 162/udp port for input to server is enabled (the default is disabled). Otherwise, the traps from the UPS(s) cannot be received. See Enabling firewall settings on page 51.

Make sure the CAT5 straight-through cables are connected from the UPSs' SNMP modules to the next available port on the customer's network. For a connectivity guide, see *Quick Start Hardware Installation: Avaya S8500 Media Server* (555-245-701). Make sure you are plugged into the correct port on the SNMP module.

The SNMP module in the UPS must be administered so it reports alarms to the media server when the hardware experiences problems. The module reports the loss of commercial power and the depletion of battery resources.

The SNMP module requires a unique IP address, which can be a customer-provided one or the Avaya-provided default one. At a minimum, the following items need to be configured:

- IP address
- Default gateway IP address
- Subnet mask
- Community name strings (get, set, trap)

Note:

For the SNMP module to properly report alarms, the IP address for the UPS must also be configured in the media server.

See Setting selected traps (alarming) on page 34 for information on which traps to set.

See the local configuration section of the User's Guide that comes with the SNMP module for the default password and the configuration commands.

Administering the SNMP modules

To administer the SNMP modules:

1. Make sure the UPS is plugged into a nonswitched electrical outlet.
2. Connect the services laptop computer (RS-232 serial port) to the DB-9 connector on the back of the SNMP module for UPS 1 using the DB-9 to DB-9 serial cable supplied with the SNMP module.

   Note:

   Avaya Terminal Emulation and HyperTerminal are supported terminal emulation applications.
3. On the services laptop open a VT-100 terminal emulation session.
4. Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control
5. Follow the instructions in the User's Guide.
6. Set the following parameters:
   - IP address and subnet mask of the UPS. (defaults are 198.152.254.239, 255.255.255.0.)
   - IP address of the trap receiver. (default is 198.152.254.200)
   - Default Gateway address of the UPS is 198.152.254.201.

   Note:

   If a Network Management System (NMS) is going to monitor the UPS, coordinate the assignment of community names with the network administrator. If an NMS is not going to monitor the UPS, set the community names to unique string values.
   - SNMP community string for Get, Set, and Trap.

SECURITY ALERT:

The **Get** and **Set**, community name strings are generally configured with default values of **Public** and **Private,** respectively. These community name strings function as passwords for their respective SNMP operation. It is always a good idea to change these community name strings to something other than the default values. If a NMS is in operation on the network, whatever these values are changed to must be coordinated with its administrator. If the defaults are left administered this could create a **serious security issue.** For example, the default Set community name string, with its widely known value of Private, could be used to shut down power to the UPS loads via an SNMP message.

7. When completed, disconnect the services laptop computer from the UPS.
8. Connect one end of a CAT5 cable to the RJ45 connector on the UPS's SNMP module and the other end to the next available port on the Ethernet switch for the control network.

Setting selected traps (alarming)

The default is to set all traps, which may result in large log entries. Therefore, only set the following traps. See the User's Guide that comes with the SNMP module for the menus and commands for setting these traps.

- UPS on Battery—Indicates AC fail with pending shutdown based on battery reserve available
- UPS in Bypass—Failure either Failed UPS or overload
- Replace battery—Failure of periodic (28-day) battery test indicating battery needs to be replaced.

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

Note:

These instruction apply only if using a new, Avaya-supplied Avaya Ethernet switch. Do not use these procedures to set traps on a non-Avaya-provided Ethernet switch.

Note:

The specific Avaya Ethernet switch model and firmware load shipped with a communication system may change over time. Therefore, this document is not specific on how to configure the SNMP subagent. Refer to the documentation that comes with the switch.

Note:

If the control network is non-dedicated (going over the customer's network), you must make sure that the 162/udp port for input to server is enabled (the default is disabled). Otherwise, the traps from the UPS(s) cannot be received. See Enabling firewall settings on page 51

The simple network management protocol (SNMP) subagent in the Avaya Ethernet switch must be administered so it can report alarms to the media server when the hardware experiences problems.

Each Avaya Ethernet switch requires a unique IP address, which can be a customer-provided one or the Avaya-provided default one. At a minimum, the following items need to be configured:

- IP address
- Subnet mask
- Trap receiver IP address
- Community string (get, set, trap)
  - Spanning tree version
  - Ethernet port speed (if applicable)

Note:

For the Ethernet switch to properly report alarms, the IP address(es) for the Ethernet switch(es) must also be configured in the media servers.

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

To administer the Ethernet switch(es):

1. Plug the Ethernet switch power cord into the back of the switch and the back of a UPS.
2. Connect the services laptop computer (RS-232 serial port) to the port labeled Console on the front of Ethernet switch 1 (CNA) using the flat cable supplied with the Avaya Ethernet switch.
3. On the services laptop open a VT-100 terminal emulation session.
4. Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
5. Follow the instructions in the Quick Start Guide.
6. Set the following parameters:
   - IP address and subnet mask of the Ethernet switch (defaults are 198.152.254.240, 255.255.0.0.)
   - IP address of the trap receiver. (default is 198.152.254.200)
   - SNMP community string for Get, Set, and Trap. (See the section on SNMP commands on the documentation CD that comes with the Avaya Ethernet switch.)

   SECURITY ALERT:

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

   Use the command **`set spantree enabled`**.

8. Set spanning tree version to rapid-spanning-tree (not the default). This command is available on Avaya P363 Ethernet switches having firmware version 4.0 or later. You must update the firmware to this version to use the command.

   Use the command **`set spantree version rapid-spanning-tree`**.

   Note:

   For more information on the Spanning Tree CLI commands, see *Installation and Configuration Guide, Avaya C360* and *Reference Guide, Avaya C360*, available at the Avaya Support Web site (http://www.avaya.com/support).

9. If IP Connect, make sure all appropriate ports on the Ethernet switch are locked to 100 speed using full duplex.
10. When completed, disconnect the services laptop computer from the Ethernet switch.
11. If two Ethernet switches are present for CNA, repeat steps 1 through 7 for the second switch.

Chapter 3: Installing Communication Manager software

A new media server comes with a blank hard drive. The Linux operating system and Release 3.0 of Avaya Communication Manager must be installed on the media server from the bootable software distribution CD-ROM.

Use the instructions in *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-701) to install the media server in the data rack. After installing the media server, you must install the software from the CD onto the hard drive.

Note:

If you are installing an S8500B Media Server to run the Expanded Meet-me Conferencing (EMMC) application, the software will be on two CDs labeled *EMMC Software Disk 1* and *EMMC Software Disk 2*.

This section covers the following tasks:

Important:

If you are installing an S8500B Media Server to run the Expanded Meet-me Conferencing (EMMC) application, follow the instructions in this section up to and including Installing Avaya Communication Manager on page 42. Then, go to *Expanded Meet-me Conferencing (EMMC) version 1.0 Installation and Troubleshooting Guide*, 04-300527 to complete the installation of the EMMC.

Clearing the ARP cache on the laptop

Depending on your laptop computer's operating system (generally Windows 2000), you may 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, then you may need to clear the cache.

1. On your laptop computer click **Start** > **Run** to open the Run dialog box.
2. Type **`command`** and press **Enter** to open a MS-DOS Command Line window.
3. Type **`arp -d 192.11.13.6`** and press **Enter** to clear the Address Resolution Protocol (ARP) cache in the laptop. This command responds with one of the following:
   - The command line prompt when the cache has been cleared.
   - The phrase: **The specified entry was not found**.

     This is returned when the specified IP address does not currently appear in the ARP cache.

Powering up the media server

To power up the media server:

1. Connect the AC power cord to the media server and to the UPS or a nonswitched outlet to power it up. If it does not power up, press the white power control button on the front of the media server.

   Note:

   You must place the CD in the drive immediately.
2. Place the CD with Avaya Communication Manager in the CD-ROM drive on the media server.

   Note:

   If you are installing an S8500B Media Server to run the Expanded Meet-me Conferencing (EMMC) application, use the CD labeled *EMMC Software Disk 1.*

Accessing the media server

To access the media server:

1. Connect the laptop to the services port (port 2 [Eth1]) on the back of the media server using a crossconnect cable.
2. Wait at least 3 minutes after powering up before starting a Telnet session to access the information on the CD.

Configuring Telnet for Windows 2000/XP

Note:

Use a telnet session to access the information on the CD.

The Microsoft Telnet application may be set to send a carriage return (CR) and line feed (LF) each time you press Enter. The installation program sees this as 2 key presses. If running Windows 2000/XP, you need to correct this before you copy the Remaster Program to the hard 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 **`display`** and press **Enter** to see the current settings. If message says

   Sending only CR

   then close the dialog box.

   If message says

   Sending both CR & LF

   then continue with step 4.
4. Type **`unset crlf`** and press **Enter**.
5. Type **`display`** and press **Enter** to verify that the settings changed. The message says

   Sending only CR
6. Close the dialog box.

Installing Avaya Communication Manager

The following steps install Avaya Communication Manager on the media server.

Note:

Use a telnet session to access the information on the CD.

1. Type **`telnet 192.11.13.6`** and press **Enter** to view the first screen.

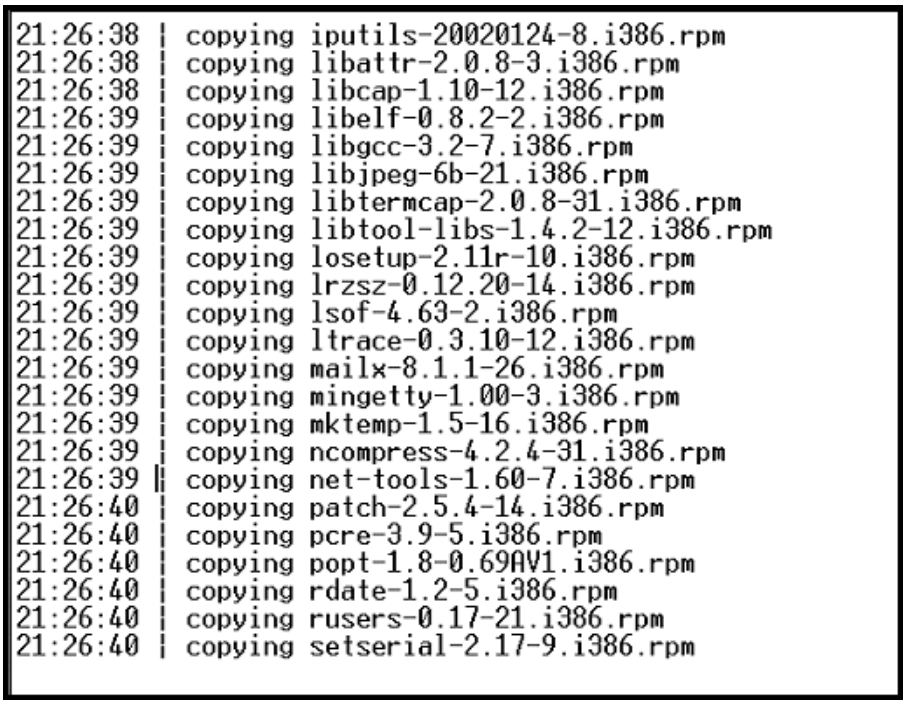
Note:

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

2. Select **Install**, make sure <OK> is highlighted, and press **Enter**.

3. On the **Select Release Version** screen, make sure the Build line and <OK> is highlighted. Press **Enter** to partition the hard drive and reformat the partitions.

   Once the drive is properly configured, the program begins the installation process and reports the progress.



These processes can take up to 20 minutes. When the media server is ready to reboot, the CD-ROM drive drawer opens. You must remove the CD from the drive at this time.

The reboot may take up to 3 minutes. The telnet session drops automatically.

Important:

If you are installing an S8500B Media Server to run the Expanded Meet-me Conferencing (EMMC) application, you are finished with this document. Continue the EMMC installation using *Expanded Meet-me Conferencing (EMMC) version 1.0 Installation and Troubleshooting Guide*, 04-300527.

Configuring the media server

After installing the Communication Manager software, you must configure the media server using the Avaya Installation Wizard.

This section covers the following tasks:

- Opening the Maintenance Web Interface on page 44
- Copying files to the media server on page 45
- Enabling Network Time Servers on page 46
- Using the Installation Wizard on page 48
- Verifying media server connection to the customer's LAN (if provided) on page 50
- Configuring the modem on page 52
- Checking LED activity on the optional dual NIC on page 53
- Disconnecting from the media server on page 54

Note:

Make sure you have the filled-out *Electronic Preinstallation Worksheet* (EPW) before beginning this process.

Note:

Make sure your networking and Web browser settings are correct. See Network configuration on page 107, of Appendix A: Accessing the media server.

Opening the Maintenance Web Interface

You can use the Maintenance Web Interface to copy files from the Services laptop to the S8500 media server, and perform other configuration tasks.

To access the media server and open the Maintenance Web Interface:

1. Launch a Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to bring up the login Web page.

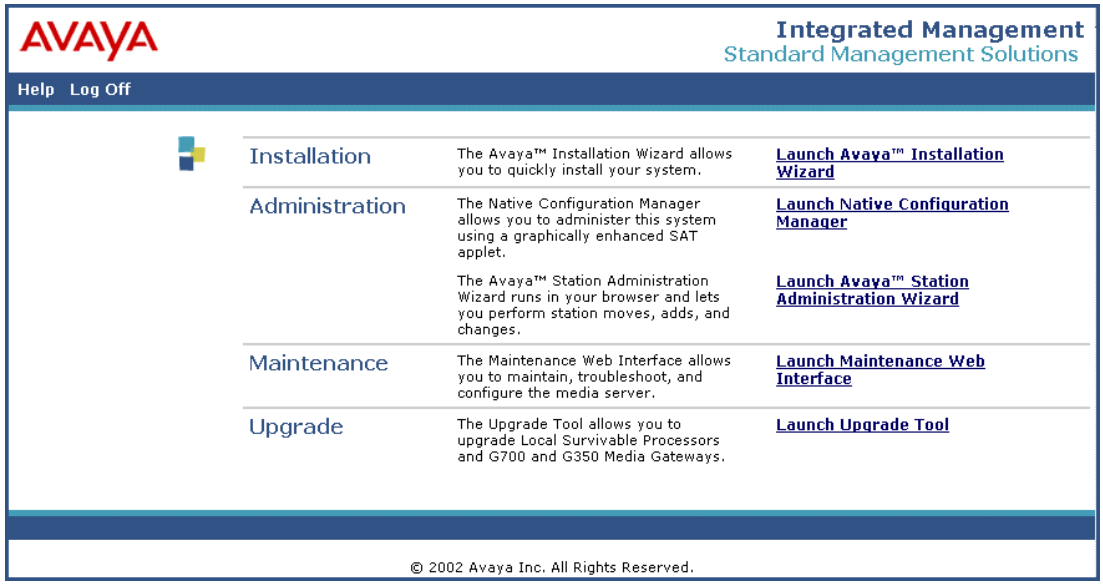
   Note:

   The first time you attempt to log in, you get a Web page asking 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 services laptop computer by following the instructions in your browser's online help.
3. Log in as **`craft`** and use the initial craft password.

4. When asked **Do you want to suppress alarms?**, select **Yes**.

   Note:

   On the initial Web page, some items may not appear at first. These include Launch Avaya Station Administration Wizard in the Administration section and the Upgrade section including Launch Upgrade Tool.



5. Click **Launch Maintenance Web Interface**.

Copying files to the media server

You can use the Maintenance Web Interface to copy license and authentication files, service packs, and SAMP update files from the Services laptop to the S8500 media server.

To copy files to the media server, complete the following steps:

1. On the Maintenance Web Interface, under **Miscellaneous**, select **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 media server.
4. Click **Download** to copy the file(s) to the media server.

   The files are automatically copied to the default file location.

Enabling Network Time Servers

Important:

Avaya strongly recommends enabling Network TIme Protocol (NTP) and configuring at least one network time server. If a network time server is not used, the Date/Time settings on the media server should be reset regularly (at least monthly), using the Maintenance Web Interface. The network time strategy should be determined by the network administrator.

Enabling Network Time Protocol allows you to specify one, two, or three network time servers to provide accurate time-of-day data to the clocks on the media servers. The network time servers, in turn, get their source timing from one of several available, highly accurate, time services on the Internet.

To use a network time server, the NTP service must be enabled. The Avaya Installation Wizard prompts for enabling the NTP service.

If you are not using the Installation Wizard, or if you want to see if NTP is enabled, follow these steps:

1. Open the Maintenance Web Interface
2. Click on the **Firewall** link under Security.
3. Enable **ntp 123/udp** in the "Output from Server" column by clicking on the checkbox.

Note:

It is not necessary to enable the "Input to Server" ntp service but if it is already enabled, you don’t have to disable it.

In the next section, Using the Installation Wizard on page 48, the Avaya Installation Wizard prompts for information about network time servers. When prompted, enter the DNS name or IP address for the primary (and secondary and tertiary, if any) network time server. If you enter a DNS name instead of an IP address for the network time server, the DNS server IP address must be specified. You are prompted for this information by the Installation Wizard.

If you are not using the Installation Wizard, the network time servers can be configured using the Configure Server function on the Maintenance Web Interface.

For detailed information about NTP, see RFC 958.

Installing the S8500 service pack, if any

If an S8500-specific service pack is required for SAMP use, install the service pack as described in this section. The procedure in this section assumes that the service pack file has been downloaded from the Avaya Support web site and copied to the S8500 media server. Once initiated, the update process should take approximately 20 minutes.

Note:

Use a telnet session to install and activate the service pack file.

The following steps activate the service pack.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **telnet 192.11.13.6** and press **Enter.**
3. Log in as either **craft** or **dadmin**.
4. Type **update_unpack** and press **Enter**.
5. Select the number corresponding to the service pack file. (For example, **00.0.339.4-xxxx.tar.gz**). Press **Enter**.
6. Type **update_show** and press **Enter** to list Communication Manager files to verify that the new service pack file was unpacked.
7. Type **update_activate *update***, where ***update*** is the release or issue number of the latest service pack file. (For example, **00.0.339.4-xxxx**. Do *not* use the .tar.gz extension at the end of the file name). Press **Enter**.

   The media server may reboot. If it reboots, it also may display the message

   ```
   /opt/ecs/sbin/drestart 2 4 command failed.
   ```

   Ignore this message. You must wait until the restart/reset completes before entering additional commands.

   The media server displays a message that the service pack was applied.
8. Type **update_show** again and press **Enter** to list Communication Manager files to verify the service pack file was activated.
9. Enter **y** in response to the question, `Commit this software?`

Using the Installation Wizard

You can configure the media server and install the license, Avaya authentication files, and software updates automatically using the Avaya Installation Wizard. You can do it two ways:

- You can import the data from the filled-out *Electronic Preinstallation Worksheet* (EPW).
- You can also type in the information manually using the filled-out EPW as a guide.

Note:

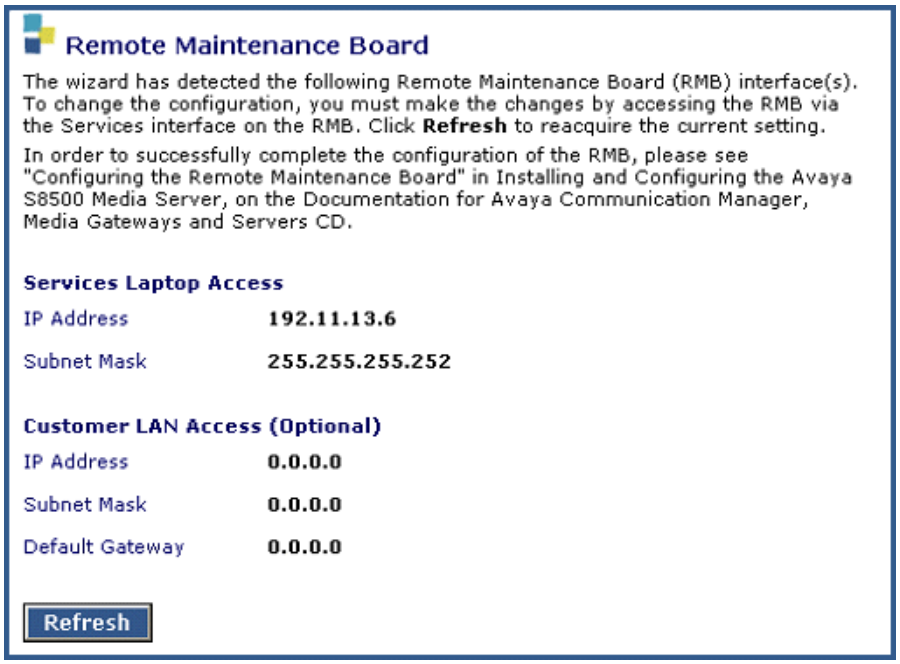
You can install the license file without being physically connected to the reference IPSI. However, you have only 30 minutes before it checks the serial number on the IPSI. To get another 30 minutes, you can restart the clock by restarting the media server. In a SAT session, type **`reset system 1`**.

1. Launch the Web browser.
2. Enter **`192.11.13.6`** and press **Enter** to bring up the login Web page.
3. Log in as **`craft`** and use the initial craft password.
4. Click **Launch Avaya Installation Wizard**.
5. Follow the Wizard prompts, using Help on each page for more information.

Configuring the RMB

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

Screen for RMB



For services laptop access:

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

The above information configures the remote maintenance board for the crossconnect cable.

For customer LAN access (optional), the 3 fields must match customer LAN

The SAMP is automatically configured within the Avaya Installation Wizard.

Installing SAMP software update, if necessary

See *The Avaya Server Availability Management Processor User Guide* for additional details on updating SAMP software.

The SAMP software may need to be updated, depending on the currently installed version. The versions that require updates should be included in your project planning information.

To update the SAMP software version, if necessary:

1. Check the SAMP software version.
   - Telnet to the S8500 and login.
   - Enter **`sampcmd samp-update status`**.

- Check the SAMP software version displayed.
- If this software version does not need to be updated, skip this procedure and continue with the next procedure, Verifying media server connection to the customer's LAN (if provided) on page 50.

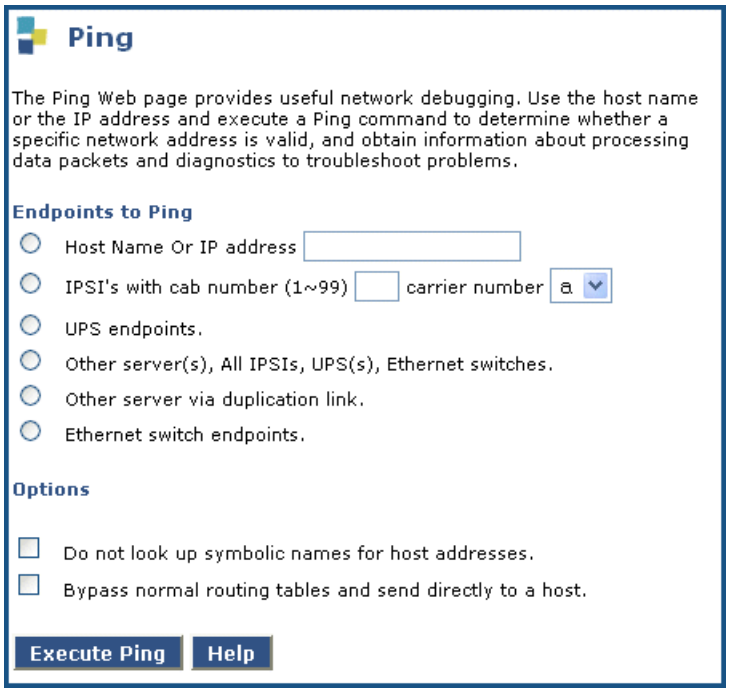
2. Copy the SAMP software update file to the S8500 using Download Files from the Maintenance Web Interface.
3. Telnet to the S8500 and login.
4. Enter **`sampupdate`** to initiate the update process.

   The update process takes approximately 5 minutes.
5. Enter **y** in response to the question, `Commit this software?`

Verifying media server connection to the customer's LAN (if provided)

To verify media server connection to the customer's LAN:

1. Under Diagnostics, click **Ping**.



2. Select **Host Name Or IP Address** and type in the IP address of a computer on the network.
3. Click **Execute Ping**.

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

If available, have a customer representative do the following test from a computer on the network:

8. Click **Start > Run** to open the **Run** dialog box.
9. Type **command** and click **OK** to open an MS-DOS command window.
10. Type **ping *serveripaddress*** and click **OK**, where ***serveripaddress*** is the IP address of the media server.
11. Verify that the ping was successful.
12. If DNS is administered, type **ping *servername*** and press **Enter**, where ***servername*** is the host name of the media server.
13. Verify that the ping was successful.

Enabling firewall settings

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

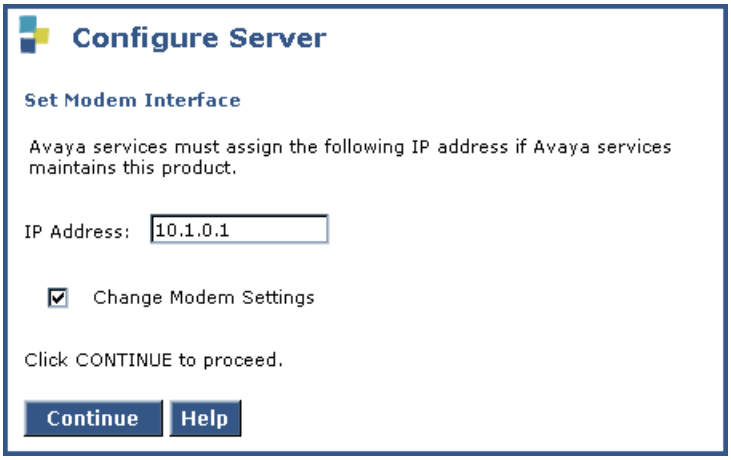
1. Under Security, click **Firewall**.
2. Click **Advanced Settings . . .** to view the second page.
3. Scroll down until you see snmptrap, port 162/udp.
4. Select the box in the **Input to Server** column (far left) next to it.

Configuring the modem

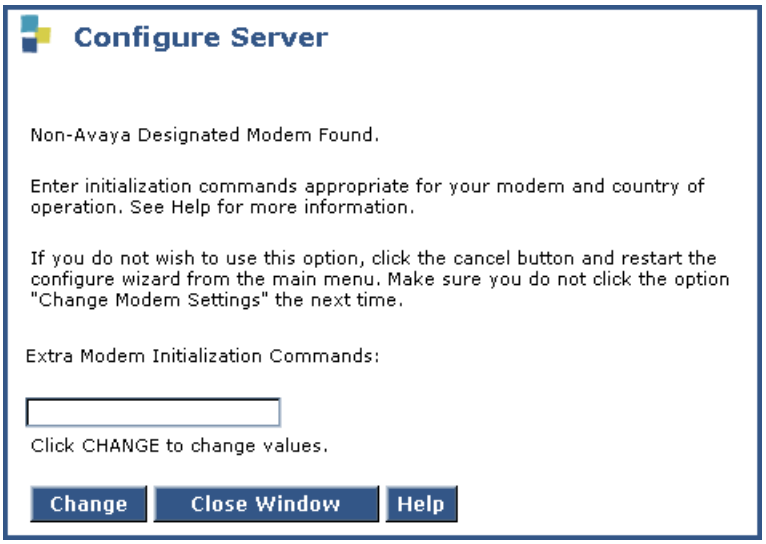
To configure the modem:

1. Under Server Configuration click **Configure Server**.
2. Click through until you get to the **Specify how you want to use this wizard** page

3. Select **Configure individual services** and click **Continue**.
4. In the left menu click **Set Modem Interface**.



5. Select the **Change Modem Setting** and click **Continue**.



6. In the **AT String** field, type the initialization commands appropriate for your modem and country of operation. Click Help for guidance on what to enter.

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

7. Click **Change**.

   The system responds with a message indicating a successfully added modem route.

8. Click **Close Window**.

Checking LED activity on the optional dual NIC

When the media server is in service, check the LEDs on each port of the dual network interface card (NIC) to make sure there is a connection (left LED) and activity (right LED). For dual-NiC LEDs see Figure 4: S8500 rear panel dual-NIC LEDs on page 54.

Figure 4: S8500 rear panel dual-NIC LEDs

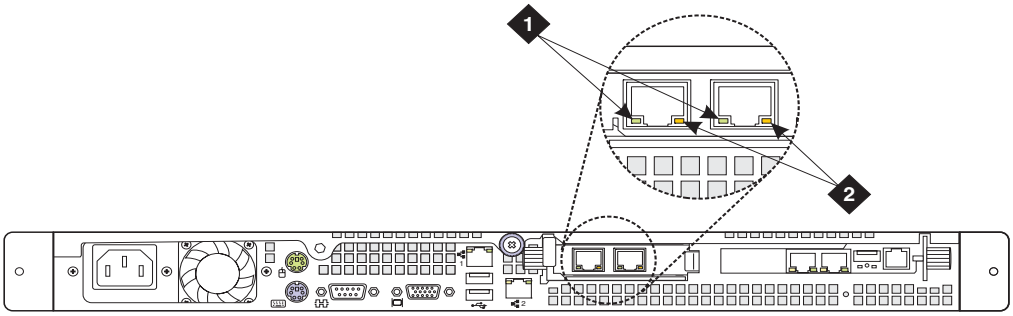


Figure notes:

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

Disconnecting from the media server

This step disconnects the laptop from the media server.

1. Unplug the crossconnect cable from the services port on the back of the media server.

Configuring the dual network interface card

This section describes the tasks required to configure the optional dual network interface card (NIC) on the Avaya S8500 Media Server. The tasks include:

- Configuring the network interface card on page 55
- Configuring the network interface card on page 55
- Testing connectivity to customer's network on page 56

Configuring the network interface card

To configure the NIC:

1. Under Server Configuration click **Configure Server**.
2. Click **Continue** through the review notices until you get to the **Specify how you want to use this Wizard** page.

3. Select **Configure Individual Services** and click **Continue**.
4. Select **Set Identities** and click **Continue**.
5. Assign Ethernet port functions using the drop-down menus for the following fields:
   - **Control Network A**: [default: Ethernet 0]
   - **Services Port**: [default: Ethernet 1]
   - **Corporate LAN**: [default: Ethernet 0]. Set this field to **Ethernet 2** to have the IPSI control on a dedicated, separate Ethernet port.
   - Unused

6. Click **Continue**.
7. Fill in the following information for Ethernet 2:
   - IP address
   - Gateway
   - Subnet mask
   - Speed
8. Verify with the customer's network administrator that the LAN hardware supports 802.1q priority tagging. If supported, select **VLAN 802.1q priority tagging**.
9. Click **Change**. The status of the configuration update appears in the window.

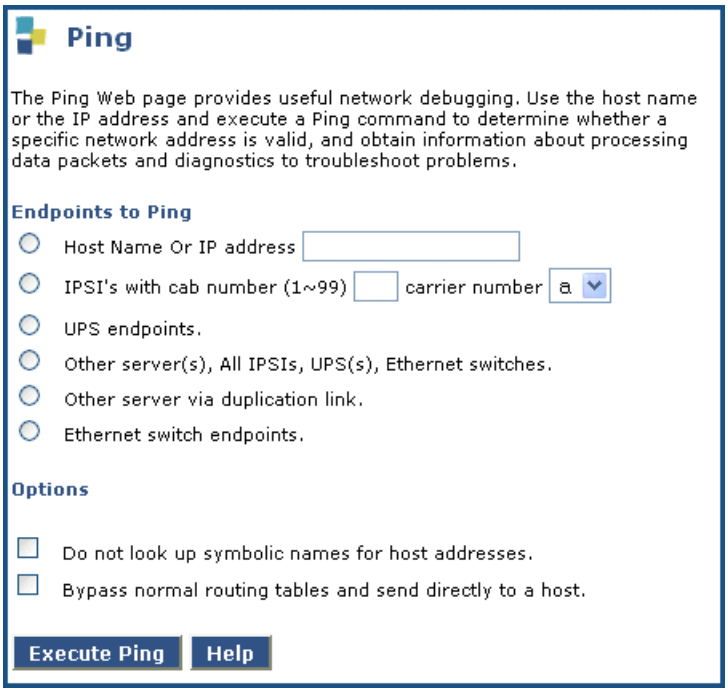
   When the update completes, the following message appears:

   Successfully configured ethernet interfaces.

Testing connectivity to customer's network

To test the connectivity to the customer's network:

1. Under Diagnostics click **Ping**.



2. Select **Host Name or IP address** and type in the IP address of a computer on the network.

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

If available, have a customer representative do the following test from a computer on their network:

8. Click **Start > Run** to open the **Run** dialog box.
9. Type **command** and click **OK** to open an MS-DOS command window.
10. Type **ping *serveripaddress*** and click **OK**, where ***serveripaddress*** is the IP address of media server.
11. Verify that the ping was successful.
12. If DNS is administered, type **ping *servername*** and press **Enter**, where ***servername*** is the host name of media server.
13. Verify that the ping was successful.

Chapter 4: Translating the IPSIs

These steps are done by issuing SAT commands on a terminal emulation program such as Avaya Native Configuration Manager, Avaya Terminal Emulation, or HyperTerminal. You also can use Avaya Site Administration, part of the Avaya Integrated Management suite, which you can purchase from Avaya.

Note:

You must use Release 2.1, update 1, or a later version of Avaya Site Administration to administer new features in Release 3.0 of Avaya Communication Manager.

Perform these tasks to customize the media server:

Starting terminal emulation

Note:

Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are supported terminal emulation applications.

These steps start terminal emulation.

1. On the services laptop, open a VT-100 terminal emulation session.
2. Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control
   - 5023 for the port
3. Log into the media server as **craft**.

Inputting translations

Contact the installation personnel responsible for translation input to download the translations.

This step downloads the translations.

1. Type **`save translation`** and press **Enter** to save the translations to the hard drive.

If the translations are not ready, you may continue with the process, entering minimal translations to verify connectivity to the port networks.

Resetting the media server

Note:

Do not reset the media server if no translations were input or if they were not entered in bulk.

This step resets the media server.

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

Adding media gateways

Note:

Do this procedure only if the translations were *not* input earlier.

Note:

A cabinet is defined as up to 5 G650 Media Gateways mounted in a rack and TDM-connected or 1 MCC1 Media Gateway.

These steps adds the media gateways to the translations.

1. Type **add cabinet number** (1 through 64) and press **Enter** for each stack of G650 Media Gateways or MCC1 Media Gateway controlled by one TN2312BP IPSI circuit pack.
2. Fill in the location and carrier type for media gateways 2(B), 3(C), 4(D), and 5(E).

```
add cabinet 1                                                  Page   1 of   1
                                    CABINET
 CABINET DESCRIPTION
                  Cabinet: 9
           Cabinet Layout: G650-rack-mount-stack
             Cabinet Type: expansion-portnetwork


                Location: 1

 Rack:               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
```

Administering the IPSIs

These steps enable the IPSI circuit packs and allow them to control the port networks.

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

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

SERVER INFORMATION

                IPSI Host Name Prefix:
       Primary Control Subnet Address: 172. 22.  0.  0*
     Secondary Control Subnet Address: 192. 11 . 13 .4*

OPTIONS

                    Switch Identifier: A
         IPSI Control of Port Networks: enabled




              NOTE: * indicates data changed on the server
```

2. Verify that the Primary Control Subnet Address is correct.

   The subnet address must match the most significant 3 octets (the first 3 groups of digits in the subnet address) of the Server IP address.

   An Asterisk (*) to the right of the **Subnet Address** field means that although a subnet address is displayed, it is not the correct one; Avaya Communication Manager does not have the subnet information. After verifying the displayed information, submit this form with or without changes to update software with the correct subnet information.

   CAUTION:

   If the information displayed in the **Subnet Address** field is not correct, it must be changed on the media server. Use the Maintenance Web Interface; under Server Configuration and Upgrades, click **Configure Server** to change the media server configuration. Then return here to perform this step.

3. Set the **Switch Identifier:** field to the switch ID letter (A through J; A is the default setting).
4. Set the **IPSI Control of Port Networks:** field to **enabled**.
5. Press **Enter** to effect the change.

Adding IPSI information

These steps add the IPSI information to the translations.

1. Type **`add ipserver-interface`** *PNnumber* and press **Enter** to add the IPSI circuit pack information.
2. For static addressing, in the **Host:** field, type in the IP address for the IPSI in the port network listed in the **Location:** field.

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

IP Control? y                                          Socket Encryption? y

                                                                Enable QoS? y

 Primary IPSI                                          QoS Parameters
 ------------                                          --------------
  Location:  1A01                                       Call Control 802.1p: 6
      Host: 172.22.22.174                              Call Control DiffServ: 46
   DHCP ID: ipsi-A01a

 Secondary IPSI
 --------------
  Location:  1B01
      Host: 172.22.22.175
   DHCP ID: ipsi-A01b
```

3. Set the **IP Control?** field to **y**.
4. Verify that all the other fields are populated.
5. Press **Enter** to effect the changes.
6. Repeat steps 1 through 5 for each port network.

Setting alarm activation level

These steps set the alarm activation level.

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

```
change system-parameters maintenance                              Page 1 of 3

                    MAINTENANCE-RELATED SYSTEM PARAMETERS

OPERATIONS SUPPORT PARAMETERS
     CPE Alarm Activation Level: none

SCHEDULED MAINTENANCE
                             Start Time: 22 : 00
                              Stop Time: 06 : 00
                        Save Translation: daily
 Update LSPs When Saving Translations: y
             Command Time-out (hours): 2
          Control Channel Interchange: no
       System Clocks/IPSI Interchange: no
```

2. In the **CPE Alarm Activation Level** field, select **none** (default), **warning**, **minor**, or **major**, depending on the level the customer wants and press **Enter** to effect the changes.
3. Repeat for each IPSI.

Installing the translation file

This step installs the translation file.

1. Type **save translation** and press **Enter** to save the translations to the hard drive.

Chapter 5: Connecting to the IPSIs

The media gateways must be installed, connected to each other, and powered up.

This chapter covers the following tasks:

At a minimum, you must program the reference IPSI and connect to it to avoid going into No License Mode. Once the IPSIs are connected to the control network, they may alarm if the firmware is not the most current. The alarm automatically goes away once the IPSI firmware is upgraded.

Connecting to the IPSIs

For a guide when connecting the CAT5 cables to the media server, refer to Figure 5: Avaya S8500 Media Server connectivity guide.

IP Connect: Connect one end of the GREEN CAT5 straight-through cable to the IPSI adapter on the back of media gateway in position A. The other end is connected to the next available port on the customer's network. If not already connected, connect it.

Direct connect: Connect a crossconnect CAT5 or better cable from the IPSI adapter to the left port (Eth2) on the dual NIC.

Figure 5: Avaya S8500 Media Server connectivity guide

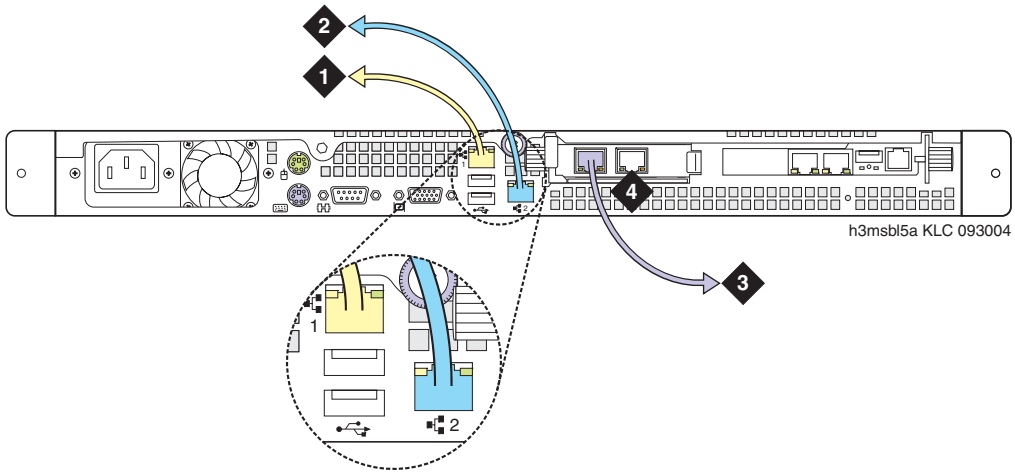


Figure notes:

1. Eth0—to customer's network if nondedicated control network. (straight-through CAT5 cable)
2. Eth1—to services laptop (cross-connect CAT5 cable)
3. Eth2—to port network if only one port network (cross-connect CAT5 cable) *or* to customer's network if dedicated control network (straight-through CAT5 cable)
4. Eth3—unused

Programming the IPSI circuit packs

IP server interface (IPSI) circuit packs get IP addresses in one of two ways:

- Using dynamic host configuration protocol (DHCP), if a dedicated (private) control network
- Using static IP addressing, if a nondedicated (public) control network through the customer's network.

Note:

Before beginning, read this procedure to familiarize yourself with it. With DHCP addressing, there are certain sequences that need to be completed before a predetermined time-out interval.

Using DHCP addressing

Important:

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

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

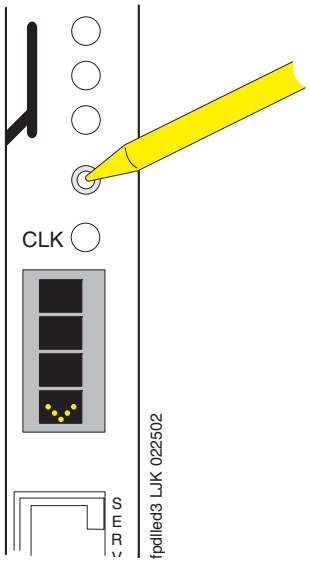
Administering the location assignment

1. Fully insert the TN2312BP IPSI circuit pack. If necessary, reseat the circuit pack to begin the programming sequence.

   Note:

   You must start the following steps within 5 seconds after inserting the circuit pack.

2. Insert a pen, golf tee, or similar object (no graphite pencil) into the recessed push button switch.



Note:

If you pass up the letter or number that you want, you must either cycle through all the letters or numbers to get to the one you want or reinsert (reseat) the circuit pack and begin again.

Setting the switch ID

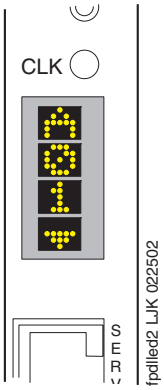
If you have only one system, the default switch ID is A. The second system would be B and so on. The switch ID is *not* the media gateway or carrier letter.

1. While the display is 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. It will flash a few times (5 seconds) then stop. The next character down begins to flash.

Setting the cabinet number

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.

1. While the first digit of the number is flashing, press the button until the correct tens digit (0 through 6) shows on the display. When the correct digit shows, stop. It flashes a few times then stops (5 seconds). The second digit begins flashing.
2. While the second digit is flashing, press the button until the correct units digit (0 through 9) shows on the display. When the correct digit shows, stop. The digit flashes a few times then stops (5 seconds).
3. All segments of the display goes dark for one second, and then the Switch ID and media gateway stack number is displayed in the top three characters of the LED display. A "V" is shown in the fourth character (bottom) of the display. When the DHCP server assigns an address to the IPSI, the center of the "V" is filled in to form the bottom half of a diamond in the display.



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

Using static addressing

Important:

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

For the IPSI circuit packs to get static IP addresses, you must administer them directly through the Ethernet port connection on the IPSI faceplate (top port). See Figure 6: Connecting directly to the IPSI.

Figure 6: Connecting directly to the IPSI

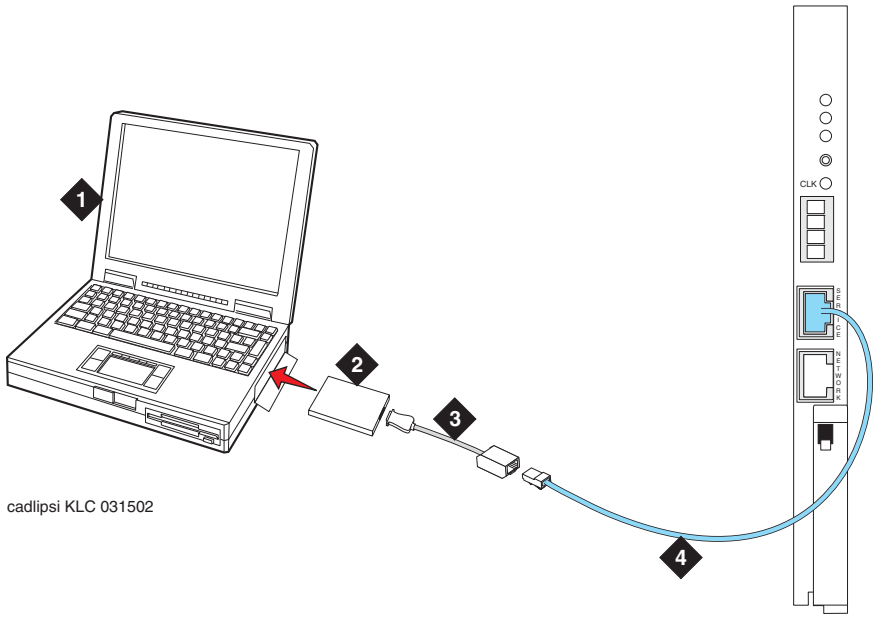


Figure notes:

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

Note:

Make sure you have the password before proceeding.

Clearing the ARP cache

Depending on your laptop computer's operating system (generally Windows 2000), you may 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, then you may need to clear the cache.

1. On your laptop computer click **Start** > **Run** to open the Run dialog box.
2. Type **command** and press **Enter** to open a MS-DOS Command Line window.

3. Type **arp -d 192.11.13.6** and press **Enter** to clear the Address Resolution Protocol (ARP) cache in the laptop. This command responds with one of the following:
   - The command line prompt when the cache has been cleared.
   - The phrase: **The specified entry was not found**.

     This is returned when the specified IP address does not currently appear in the ARP cache.

Logging into the IPSI

The following steps logs you into the IPSI.

1. Type **telnet 192.11.13.6** and press **Enter** to open the Telnet window and connect to the IPSI

   Prompt = [IPSI]:

   Note:

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

2. Type **ipsilogin** and press **Enter** (abbreviated command = **il)**.

   Note:

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

3. Log in as **craft**.

   Prompt = [IPADMIN]:

Setting the control interface

The following steps set the control interface.

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

3. 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]:
```

4. Enter **quit** to save the changes and exit the IPSI session.
5. Telnet to **192.11.13.6** and login.
6. Enter **show control interface**.
   The IP address, subnet mask, and default gateway information are displayed.
   Verify that the proper information was entered.
7. If a default gateway is used, enter the gateway IP address using **set control gateway *gatewayaddr***, where ***gatewayaddr*** is the customer-provided IP address for their gateway.
8. Enter **quit** to save the changes and exit the IPSI session.
9. Telnet to **192.11.13.6** and login.
10. Use **show control interface** to verify the administration.
11. Type **exit** and press **Enter** to see the changes.

Setting the VLAN and diffserv parameters

The following steps sets the VLAN and diffserv parameters.

1. Log back in as **craft**.
2. Enter show **qos** to display the quality of service values.

3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

   Note:

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

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

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

   Important:

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

Resetting the IPSI

The following steps resets the IPSI and ends the administration session.

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

   Note:

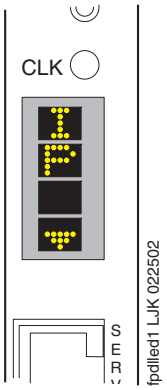
   Resetting the IPSI terminates the administration session. If further administration is required, start a new telnet session to the IPSI.

   Note:

   Control network settings (IP address, subnet mask, and gateway) become effective when you exit the IPADMIN session.

2. Disconnect the laptop from the faceplate.
3. Check the LCD. Verify that it has an I P with a filled-in V showing at the bottom. (See Figure 7: LED display showing that the IPSI has a static IP address)

Figure 7: LED display showing that the IPSI has a static IP address



Note:

Clear the ARP cache on the laptop before connecting to another IPSI. If the cache is not cleared the laptop appears to hang and does not connect to the next IPSI. See Clearing the ARP cache on page 70.

4. Repeat for each IPSI circuit pack.

Verifying connectivity to media server

These steps verify connectivity to the media server.

1. If not already open, open a browser and log in as **craft**.
2. Click **Launch Maintenance Web Interface**.
3. Under Diagnostics, 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 IPSIs are translated

These steps verify that the IPSIs are translated.

1. Log into the media server using a terminal emulation application.
2. Type **`list ipserver-interface`** and press **Enter**.
3. Verify that all ISPI circuit packs are translated.

Upgrading IPSI firmware version (if necessary)

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

These steps upgrade the IPSI firmware version.

1. Under IPSI Firmware Upgrades click **IPSI Version**.
2. Select **Query All** and click **View IPSI Version**.
3. Verify the firmware release for each TN2312BP IPSI. If an upgrade is required, follow the procedures in *Upgrading Software and Firmware—Avaya S8500 Media Server* (555-245-111), Upgrading IPSI Firmware.

Enabling control of IPSIs

Note:

Make sure the IPSIs have the same, current firmware.

These steps enable the IPSI circuit packs and allow them to control the port networks.

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

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

SERVER INFORMATION

                IPSI Host Name Prefix:
       Primary Control Subnet Address: 172. 22.  0.  0
     Secondary Control Subnet Address:    .   .   .

OPTIONS

                    Switch Identifier: A
        IPSI Control of Port Networks: enabled
```

2. Make sure the **IPSI Control of Port Networks:** field is set to **enabled**.
3. Press **Enter** to effect the changes.

Verifying license status

These steps verify the license status.

1. Under Security, click **License File** and verify that the license mode is now normal.

Reusing a TN2312AP/BP circuit pack

Note:

This is not part of a normal installation process.

On occasion a customer may want to reuse a TN2312AP or TN2312BP circuit pack that was previously programmed for DHCP or static addressing. You must erase the existing programming before reprogramming it. Failure to do this may result in serious network problems.

For information on erasing the programming, go to the *Maintenance Procedures for Avaya Communication Manager 3.0, Media Gateways and Servers* (03-300432).

Chapter 6: Completing the installation administration

This section covers the following tasks:

Verifying translations

These steps verify translations.

1. Type **`list configuration all`** and press **Enter** to view all the administered circuit packs in the system.
2. Type **`list ipsi`** and press **Enter** to verify the location of the IPSI circuit packs.
3. Check the administration status on the following items:
   - **`list station`**
   - **`list trunk-group`**
   - **`list hunt-group`**

   Note:

   Even though you set the date, time, and time zone through the Web interface on the media server, you also must set the daylight savings time rules and locations and verify the date and time through SAT commands.

Setting daylight savings time rules

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 them 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. It also specifies the increment at which to transition.

Note:

The default daylight savings rule is **0**, meaning no daylight savings transition.

1. Type **`change daylight-savings-rules`** and press **Enter**.

```
change daylight-savings-rules                                  Page   1 of   2
                        DAYLIGHT SAVINGS RULES

 Rule          Change Day                 Month  Date   Time    Increment

  0: No Daylight Savings

  1: Start: first Sunday     on or after April     1   at 02:00   01:00
     Stop: first Sunday      on or after October   25  at 02:00
  2: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  3: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  4: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  5: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  6: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  7: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
```

2. In the **Change Day**, **Month**, **Date**, **Time**, and **Increment** fields, 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.

Note:

You can change any rule except rule 0 (zero). You cannot delete a daylight savings rule if it is in use on either the **Locations** or **Date and Time** screens.

3. When done, press **Enter** to effect the changes.

Setting locations (if necessary)

After you set the daylight savings rules, you must set the locations for all media gateways (cabinets). It is possible to have media gateways in different time zones.

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**.
3. Type the information in the various fields for each media gateway.

   Note:

   In the **Name** field for location 1, call the media gateway (cabinet) Main.

4. Press **Enter** to effect the changes.

Verifying date and time

These steps 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: November
           Day of the Month: 8               Year: 2002

        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 time are correct.
3. Verify that the correct rule (number) is displayed in the **Daylight Savings Rule** field.
4. If correct, press **Cancel**.
5. If not, go to the Maintenance Web Interface.
6. Under Server, click **Set Server Time/Timezone**.
7. Verify that the date and time are correct. If not, set it here.
8. Repeat steps 1 through 3.

Resolving alarms

To resolve alarms:

1. Under Alarms click **Current Alarms**.
2. Select the server alarms to be cleared and click **Clear**.
3. Resolve any major alarms using SAT commands and a terminal emulation application, such as Native Configuration Manager or MS HyperTerminal.

Backing up files to the compact flash media

These steps back up files to the compact flash media.

1. Connect the compact flash drive to the top USB port on the front of the media server.
2. Insert a 128-Mb compact flash media into the top right slot of the drive.

   Note:

   The industrial grade compact flash media provides improved data integrity and reliability, enhanced durability, and extreme endurance. For these reasons Avaya recommends the use of an industrial grade compact flash. To read more about the industrial grade compact flash, see the *Hardware Guide for Avaya Communication Manager* (555-245-207).

   Note:

   You must format the compact flash media before writing to it.
3. Under Data Backup/Restore click **Backup Now**.
4. Select all applicable data sets.
5. Select either Local PC Card and Format PC Card, or Format PC Card (the second such selection further down the screen).

   Use Local PC Card and Format PC Card to format the PC card and back up the data onto it.

   Use Format PC Card to format new cards or to overwrite an existing card.

   Note:

   Customer’s may want to back up using another method.
6. Click **Start Backup.** You are notified when the format is completed (approximately 10 seconds).

   Note:

   Clicking on **Start Backup** without media in the compact flash drive results in an error. To continue with the backup, unplug the drive, insert the formatted media into the right top slot, and plug the drive back into the USB port.
7. Click **Backup Status** to view the status of the backup.

Telneting to media server

Enabling alarms uses Linux commands through Telnet.

The following steps start a telnet session.

1. Click **Start > Run** to open the **Run** dialog box
2. Type **`telnet 192.11.13.6`** and press **Enter**.
3. Log in as **`craft`** or **`dadmin`**.

Enabling alarms

To INADS via modem

These steps enable alarms to INADS via the modem.

1. Type **`almenable -d b`** and press **Enter**.
2. Type **`almenable`** and press **Enter** to verify that the alarms are enabled.

To INADS via SNMP

Note:

Do these steps only if a Secure Service Gateway (SSG) is being installed.

These steps enable alarms to INADS via SNMP.

1. 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 required by the SSG device.
2. Type **`almsnmpconf`** and press **Enter**.

   Verify that the correct information was entered.
3. At the prompt, type **`almenable -s y`** and press **Enter**.
4. Type **`almenable`** and press **Enter**.

   Verify that the SNMP alarm origination is enabled. If used, verify that alarm origination via modem is still enabled.
5. Log off.

Registering the system

Follow the existing process and procedures to register the media server.

Before leaving the site

Let customers know what the default LAN security settings are; they may want to change them after installation. Make sure they are aware that if the following items are not enabled, they will not have remote access to the media server:

- telnet—no Telnet access
- https—no Maintenance Web Interface access
- def-sat—no SAT command access

Chapter 7: Installing the media gateways

In a new installation, the Avaya S8500 Media Server works with only the Avaya G650 Media Gateway.

In a migration the media server works with the following Avaya Media Gateways:

- MCC1
- SCC1
- G600
- CMC1

In addition, the media servers work with Avaya G350 and G700 Media Gateways. The media servers work with the G650 Media Gateway only when the gateway has a TN799DP C-LAN circuit pack installed. These gateways are treated as endpoints off the TN799DP.

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

For information on installing media gateways, see

- *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 G350 Media Gateway* (03-300148)
- *Installation of the Avaya G350 Media Gateway* (555-245-104)
- *Quick Start for Hardware Installation: Avaya S8300 Media Server and Avaya G700 Media Gateway* (555-233-150)
- *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server* (555-234-100)

Chapter 8: Testing the media server installation

This chapter provides tests for the control network, including

- reviewing the status of the configuration.
- testing the IPSI circuit packs.

In addition, it provides information on the LED status indicators for the media servers, Avaya Ethernet switch(es), uninterruptible power supplies (UPSs), and different circuit packs. See LED indicators on page 91.

Note:

Circuit pack positions are usually given by cabinet, and slot. They may also be given by port. The term cabinet refers to five G650 Media Gateway TDM-cabled together in a rack, making up one port network. A port network is defined as a group of media gateways connected together with one TDM bus.

Perform these tasks to test the configuration:

CAUTION:

To prevent unnecessary trouble tickets, do not enable the alarms (Alarm Origination feature) until all installation and administration procedures are completed.

Testing the TN2312BP IPSI circuit pack

Note:

Do these steps using a SAT session

These steps test the TN2312BP IPSI circuit pack.

1. Type **`test ipserver-interface UUC`** and press **Enter** to test all clock and packet interface components within the IPSI circuit pack.
2. Verify the screen displays **Test Results** screen similar to Figure 8: Sample IPSI 01A test results screen—page 1.

Figure 8: Sample IPSI 01A test results screen—page 1

```
test ipserver-interface 1a                                          Page   1

                                TEST RESULTS

Port        Maintenance Name  Alt. Name Test No. Result           Error Code

01A         TONE-BD                     46       PASS
01A         TONE-BD                     52       PASS

               press CANCEL to quit --  press NEXT PAGE to continue
```

Testing the license file

CAUTION:

Wait at least 30 minutes after you install the license before you do the test.

Note:

Do these steps using a SAT session

These steps test the license file.

1. Type **`test license [short | long]`** and press **Enter**.
2. Verify the screen displays a **Test Results** screen similar to Figure 9: Sample test results screen for test license.

Figure 9: Sample test results screen for test license

```
test license

                                TEST RESULTS

Port        Maintenance Name  Alt. Name Test No. Result           Error Code

            LIC-ERR                     1484     PASS
```

LED indicators

See the *Maintenance Alarms for Avaya Communication Manager 3.0, Media Gateways and Servers* (03-300430) for detailed alarm and LED descriptions. If a maintenance object begins to fail some periodic tests, the media server generates an alarm.

The media server identifies three levels of alarms:

1. Major Alarms—Failures that cause critical degradation of service and require immediate attention.
2. Minor Alarms—Failures that cause some degradation of service, but do not cause a critical portion of the configuration to be inoperable. This condition requires action, but its consequences are not immediate. Problems might be impaired service to a few trunks or stations or interfering with one feature across the entire configuration.
3. Warning Alarms—Failures that cause no significant degradation of service or failures in equipment external to the configuration. Warning alarms are not reported to the attendant console or **INADS**.

Alarms are communicated to users and technicians by entries in the alarm and system logs and the lighting of **LED**s located on the media server.

More detailed information is available here for:

1. Avaya S8500 Media Server LEDs on page 92
2. Avaya S8500 Media Server LEDs on page 92

- Avaya Ethernet switch LEDs on page 94
- Uninterruptible power supply LEDs on page 97
- IPSI LEDs on page 97

Avaya S8500 Media Server LEDs

For information on the various LEDs, see Figure 10: Front of the Avaya S8500 Media Server.

Figure 10: Front of the Avaya S8500 Media Server

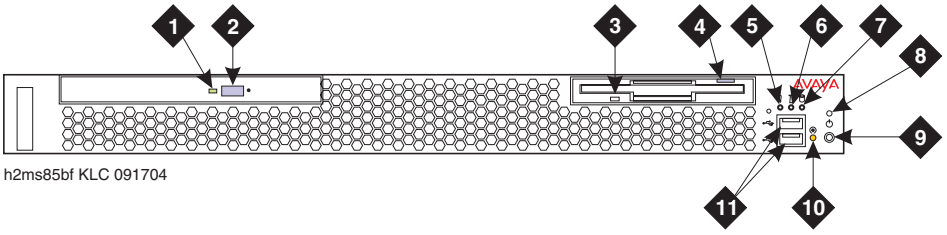


Table 5: Description of controls and LEDs

Control/LED	Description
1: CD-ROM drive activity LED	When lit, the CD-ROM drive is in use.
2: CD eject button	Press to release a CD from the CD-ROM drive.
3: Diskette drive activity LED	When lit, the diskette drive is in use.
4: Diskette eject button	Press to release a diskette from the diskette drive.
5: System error LED	When lit, a system error has occurred.
6: System locator LED	Use this blue LED to visually locate the media server if it is in a location with numerous other media servers.
7: Hard disk drive activity LED	When flashing, a hard disk drive is in use.
8: Power on LED	When lit and not flashing, the media server is turned on. When flashing, the media server is turned off and still connected to the an ac power source. When off, ac power is not present, or the power supply or the LED itself has failed.
9: Power control button	Press to turn the media server on and off manually.
10: Reset button	Press to reset the media server and run the power-on self-test (POST). You might have to use a pen or the end of a straightened paper clip to press the button.
11: USB connections for the Compac Flash drive	

Figure 11: S8500 Media Server, rear view

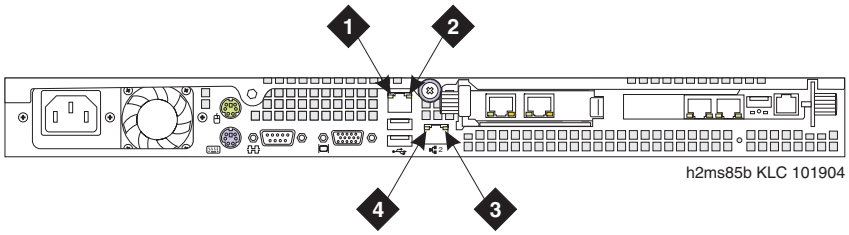


Table 6: Description of LEDs

Control/LED	Description
1. LAN 1 transmit/receive activity LED	This LED is on the Ethernet connector. When lit, it indicates that there is activity between the media server and the network.
2. LAN 1 speed 1 Gbps LED	This LED is on the Ethernet connector. When lit, it indicates that the Ethernet network speed is 1 Gbps. When off, it indicates that the Ethernet network speed is 10 Mbps or 100 Mbps.
3: LAN 2 speed 1 Gbps LED	This LED is on the Ethernet connector. When lit, it indicates that the Ethernet network speed is 1 Gbps. When off, it indicates that the Ethernet network speed is 10 Mbps or 100 Mbps.
4: LAN 2 transmit/receive activity LED	This LED is on the Ethernet connector. When lit, it indicates that there is activity between the media server and the network.

The Avaya S8500 Media Server has five LEDs on the front and four LEDs in the back. The following is a brief description of the function of each LED:

- Ethernet 1 link (GREEN): Lights when the speed of the Ethernet LAN is 1000BASE-T. The green LED will be off when the speed of the Ethernet LAN is 10/100BASE-T.
- Ethernet 2 activity (GREEN): Blinks when there is an active 10/100/1000BASE-T connection.
- Ethernet 2 link (GREEN): Lights when the speed of the Ethernet LAN is 1000BASE-T. The GREEN LED will be off when the speed of the Ethernet LAN is 10/100BASE-T.

There are no LEDs on the SAMP.

Avaya Ethernet switch LEDs

The C360 series converged, stackable, Ethernet switches include:

- 24-port **C363T**
- 24-port power over Ethernet **C363T-PWR**
- 48-port **C364T**
- 48-port power over Ethernet **C364T-PWR**

The front panel of these switches has one port LED associated with each port, three system status LEDs, and seven port function LEDs. The 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.

The following table lists the system and port function LEDs.

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

See the documentation shipped with the Ethernet switch for the interpretation of the on/off/blinking states of the LEDs.

Avaya S8500 Media Server LEDs

LEDs on the Avaya S8500 Media Server are described in Figure 12: Front of the Avaya S8500 Media Server.

Figure 12: Front of the Avaya S8500 Media Server

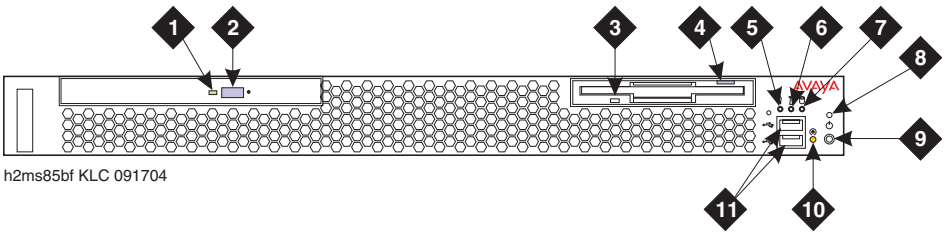


Table 7: Description of controls and LEDs

Control/LED	Description
1: CD-ROM drive activity LED	When lit, the CD-ROM drive is in use.
2: CD eject button	Press to release a CD from the CD-ROM drive.
3: Diskette drive activity LED	When lit, the diskette drive is in use.
4: Diskette eject button	Press to release a diskette from the diskette drive.
5: System error LED	When lit, a system error has occurred.
6: System locator LED	Use this blue LED to visually locate the media server if it is in a location with numerous other media servers.
7: Hard disk drive activity LED	When flashing, a hard disk drive is in use.
8: Power on LED	When lit and not flashing, the media server is turned on. When flashing, the media server is turned off and still connected to the an ac power source. When off, ac power is not present, or the power supply or the LED itself has failed.
9: Power control button	Press to turn the media server on and off manually.
10: Reset button	Press to reset the media server and run the power-on self-test (POST). You might have to use a pen or the end of a straightened paper clip to press the button.
11: USB connections for the Compac Flash drive	

Figure 13: S8500 Media Server, rear view

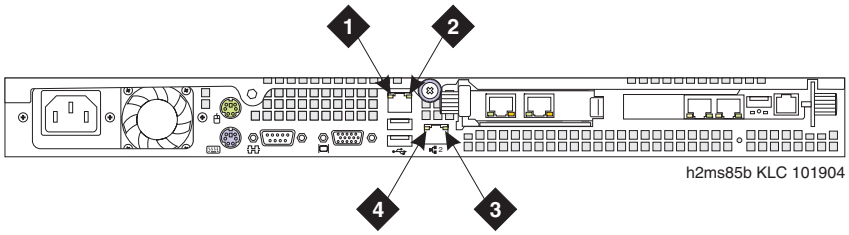


Table 8: Description of LEDs

Control/LED	Description
1. LAN 1 transmit/receive activity LED	This LED is on the Ethernet connector. When lit, it indicates that there is activity between the media server and the network.
2. LAN 1 speed 1 Gbps LED	This LED is on the Ethernet connector. When lit, it indicates that the Ethernet network speed is 1 Gbps. When off, it indicates that the Ethernet network speed is 10 Mbps or 100 Mbps.
3: LAN 2 speed 1 Gbps LED	This LED is on the Ethernet connector. When lit, it indicates that the Ethernet network speed is 1 Gbps. When off, it indicates that the Ethernet network speed is 10 Mbps or 100 Mbps.
4: LAN 2 transmit/receive activity LED	This LED is on the Ethernet connector. When lit, it indicates that there is activity between the media server and the network.

The Avaya S8500 Media Server has five LEDs on the front and four LEDs in the back. The following is a brief description of the function of each LED:

- Ethernet 1 link (GREEN): Lights when the speed of the Ethernet LAN is 1000BASE-T. The green LED will be off when the speed of the Ethernet LAN is 10/100BASE-T.
- Ethernet 2 activity (GREEN): Blinks when there is an active 10/100/1000BASE-T connection.
- Ethernet 2 link (GREEN): Lights when the speed of the Ethernet LAN is 1000BASE-T. The GREEN LED will be off when the speed of the Ethernet LAN is 10/100BASE-T.

There are no LEDs on the SAMP.

Uninterruptible power supply LEDs

The Powerware uninterruptible power supply (UPS) front panel has the LEDs shown in Figure 14: LEDs on Powerware 9125 UPS.

Figure 14: LEDs on Powerware 9125 UPS

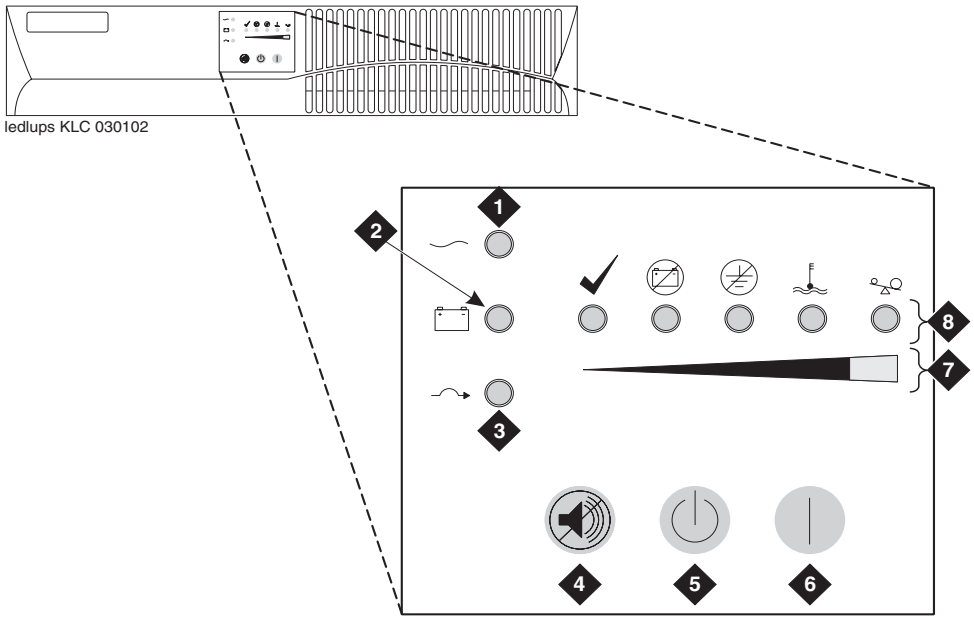


Figure notes:

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

After plugging in the UPS, all the LEDs flash briefly. After a self test, the Normal mode LED flashes, indicating that the UPS is in Standby mode.

For more information on the LEDs, see the UPS user's guide that comes with the Powerware UPS.

IPSI LEDs

The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack LEDs are shown in Figure 15: TN2312BP circuit pack faceplate on page 98). It also has a programmable LED display to indicate whether its IP address is dynamic (shows media gateway location) or static (shows I P). See Figure 16: LED display on the IPSI circuit pack—static address on page 99.

Figure 15: TN2312BP circuit pack faceplate

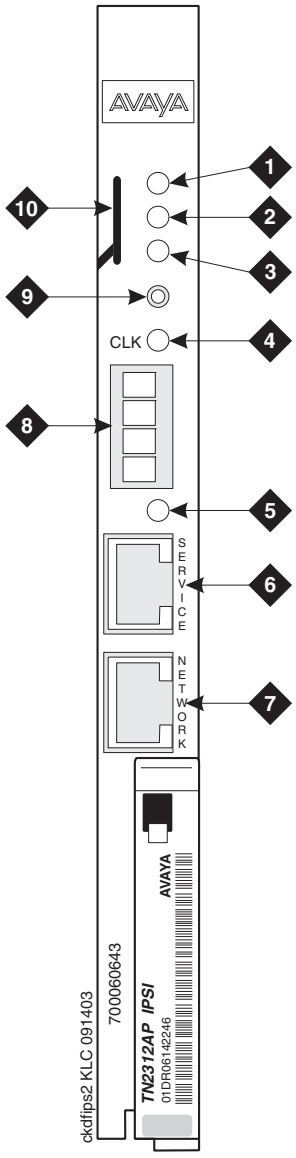


Figure notes:

1. Red LED
2. Green LED
3. Amber LED
4. Yellow LED (Tone Clock status)
5. Emergency Transfer LED
6. Services RJ45 connector
7. Network Control RJ45 connector
8. 4-character LED display
9. Pushbutton switch
10. Slot for maintenance cable

Figure 16: LED display on the IPSI circuit pack—static address

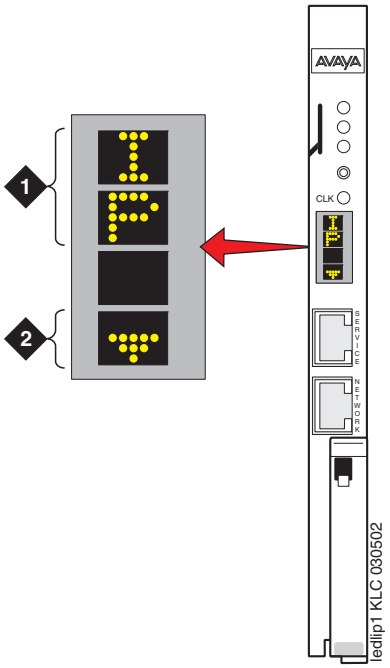
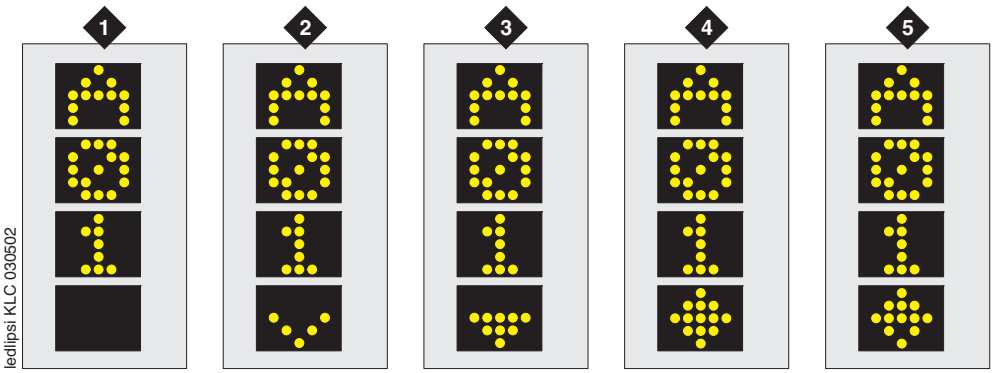


Figure notes:

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

The display also indicates connectivity (see Figure 17: LED display indicating connectivity status—DHCP address on page 100).

Figure 17: LED display indicating connectivity status—DHCP address



Connectivity status	1	2	3	4	5
IPSI is connected to media server	no	yes	yes	yes	yes
IPSI has an IP address	no	no	yes	yes	no
Laptop computer is connected to IPSI services port	no	no	no	yes	yes

Appendix A: Accessing the media server

To administer the media server, you must be able to access it. Personal computers and services laptop computers equipped with a network interface card (NIC), a terminal emulation program, and a Web browser are the supported access points for accessing the media server for initial configuration, aftermarket additions, and continuing maintenance.

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

This section covers the following sections:

Connecting to the media server directly

You access the media server directly by plugging a laptop computer into the services port (port 2 [Eth1]) on the media server. See Figure 18: Services laptop computer connected directly to the S8500 Media Server on page 102 or Figure 19: Services laptop computer connected directly to the S8500 Media Server on page 103. The computer used for accessing the media server must have the following minimum specifications:

- Windows 2000/XP operating system
- 32-MB RAM
- 40-MB available disk space
- RS-232 port connector
- Network interface card (NIC) with a 10/100BaseT Ethernet interface
- 10/100 BaseT Ethernet, category 5 (or better), crossconnect cable with an RJ45 connector on each end (MDI to MDI-X)
- CD-ROM drive

Plug one end of the CAT5 cable into the services access port, which defaults to port 2 (Eth1), on the back of the media server and the other end into the NIC on your computer. (You may need a NIC adapter.)

You also must configure your network connection. For specific information, see Network configuration on page 107.

The network connection for the computer is

- IP address: 192.11.13.5
- Subnet mask: 255.255.255.252

Figure 18: Services laptop computer connected directly to the S8500 Media Server

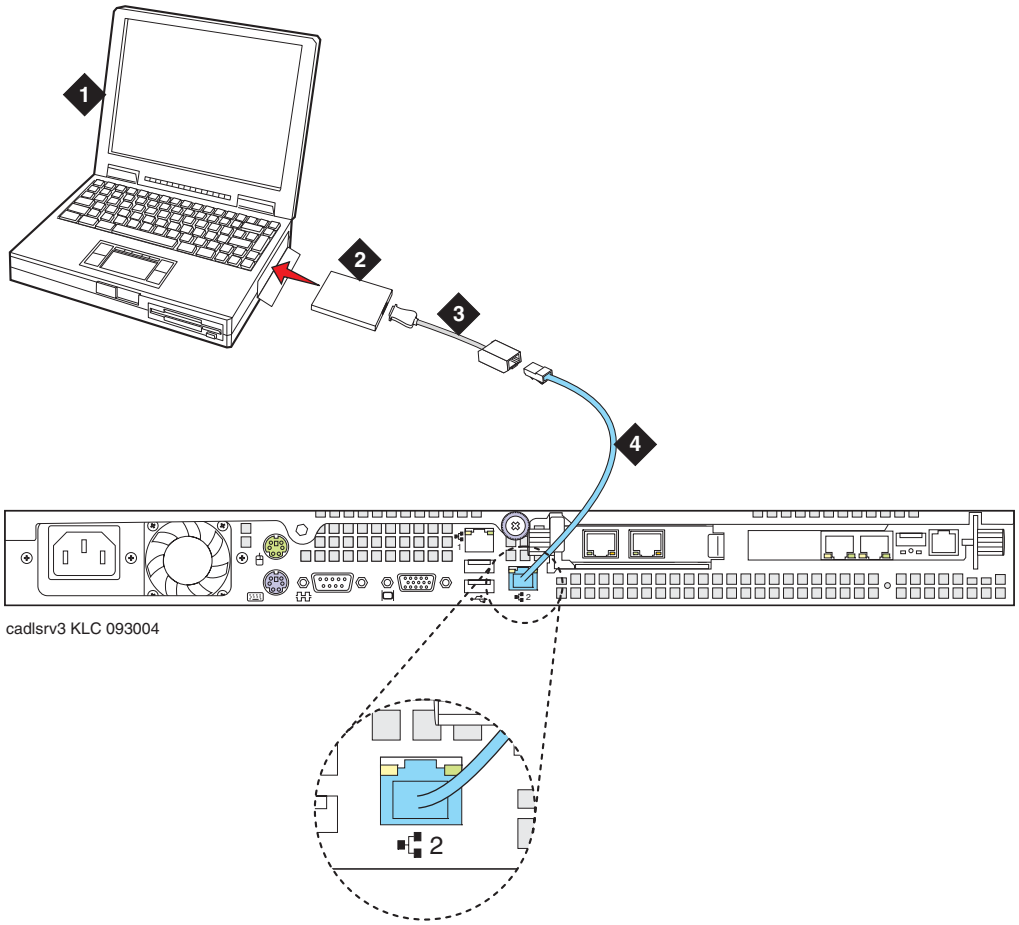


Figure notes:

1. Services laptop
2. Network interface card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 crossconnect cable

Figure 19: Services laptop computer connected directly to the S8500 Media Server

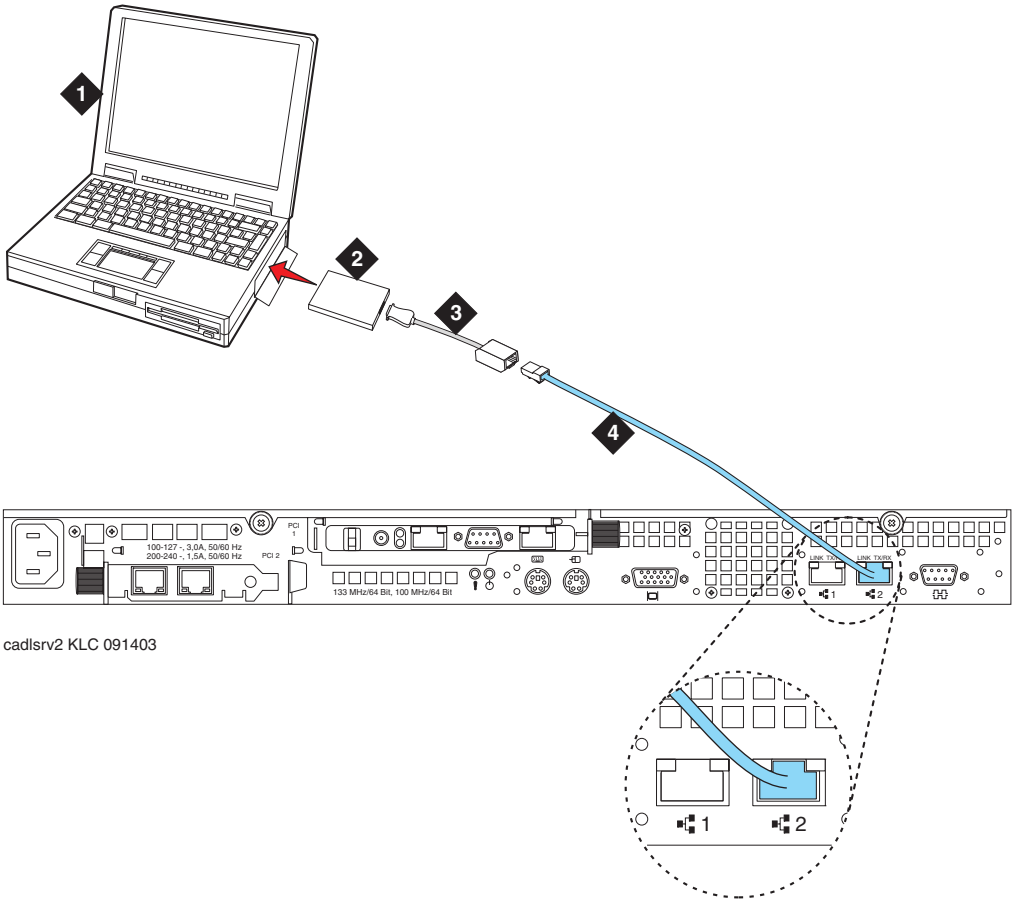


Figure notes:

1. Services laptop
2. Network interface card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 crossconnect cable

Once connected, you can administer the media server using these interfaces:

- Maintenance Web Interface for server-specific administration.
- A command line interface in a Telnet or terminal emulation application for Linux and SAT commands (usable on the active media server only).

See Accessing the Maintenance Web Interface on page 106 for more details.

Connecting to the media server remotely over the network

You can access the media server from any computer connected through the LAN. However, make sure the LAN security settings allow remote access.

To access the media server, open a Web browser or a terminal emulation application. In the address field, type in the IP address or DNS host name assigned to the media server you want to access.

Connecting to the media server remotely over a modem

This section covers the following tasks:

- Setting up a dial-up connection on page 105
- Dialing up to the media server on page 105
- Accessing the Maintenance Web Interface on page 106
- Using the command line interface on page 106

Note:

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

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

On the S8500 Media Server, you access the media server through the remote maintenance board installed in the media server. For information on accessing the SAMP, see the *Avaya Server Availability Management Processor User Guide* (03-300322).

Setting up a dial-up connection

To use a computer modem, you first must set it up through your dial-up connection.

1. Launch the dial-up connection program, which varies depending on your operating system. Generally, you can access them through My Computer or Control Panel folders. See your computer's help system for specific information.
2. Double-click **Make New Connection** to open the New Connection wizard.
3. Within the wizard, and 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.
   - Type in the appropriate telephone number to access the active server. See the filled-out job aid titled *Electronic Preinstallation Worksheet* for the customer-supplied telephone number(s).
   - Under Advanced, select **PPP** and log on manually. You may have to type in a user name and password, depending on whether or not the media server you are dialing into has a non-null CHAP secret key. Use **craft** (ignore the password field).

Dialing up to the media server

To dial up, click the connection name or icon, if created. Once you are connected:

1. When prompted, enter your remote access login name and password.
2. When the **Start PPP now!** message appears, click **Done**. When you see the Connection Complete dialog box, your computer is connected to the media server.
3. To open a Telnet session, click **Start** > **Run** to open the **Run** dialog box.
4. In the Run dialog box, type **`telnet IPaddress`** and click **OK**, where ***`IPaddress`*** is the address of the actual active media server.

Accessing the Maintenance Web Interface

You can access the Maintenance Web Interface either by connecting directly to the services port (port 2 [Eth1]) on the media server (see Figure 19: Services laptop computer connected directly to the S8500 Media Server on page 103) or connecting over the customer's network. The only browser supported is MS Internet Explorer 5.5 or 6.0.

When connected *directly* to the media server, you must disable all proxy servers. See Browser settings on page 108 for instructions.

1. Open the MS Internet Explorer Web browser.
   - If a direct connection, in the **Address** field, type `192.11.13.6`.
   - If a remote connection, in the **Address** field, type in the IP address or DNS host name of the media server.
2. When prompted, log in.

Using the command line interface

Telnet: To open a Telnet window session.

1. Click **Start** > **Run** to open the **Run** dialog box.
   - If a direct connection, type `telnet 192.11.13.6` and click **OK**.
   - If a remote connection, type in the IP address of the media server.
2. When prompted, log in.

Terminal Emulation: To use a command line interface in a terminal emulation window open your terminal emulation application. The terminal emulation program port settings must be configured as follows:

- 115200 baud
- 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 supported.

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

Logins

Initial configuration and upgrades by an Avaya field tech or business partner requires a services login, such as craft or dadmin. If an Avaya field tech, you can use a unique password assigned to that customer's system.

After installing the Avaya authentication file, Avaya Communication Manager has a password for the craft login that is unique to the customer's system and available when connected directly to the media server. To bypass the ASG challenge and response, use this password the next time you log in as **craft**. Every other means of craft access still require an ASG challenge and response. The revised password is recorded by RFA and is obtained from ASG Conversant at 1-800-248-1234 or 1-720-444-5557.

Customer's can set up their own logins for accessing Avaya's media servers. See the *Avaya Communication Manager Basic Administration Quick Reference* (03-300363) for specific information. You must have superuser permission to create or change logins and passwords.

Note:

When assigning login IDs, do not start them with a number.

Network configuration

Note:

Write down the original settings in case you need to change them back.

A new network connection must be configured as follows:

Note:

These instructions are for Windows 2000/XP only.

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

   Windows 2000/XP should have automatically detected the Ethernet card in your system and created a LAN connection for you. More than one connection may appear.

2. Right-click on the correct **Local Area Connection** and left-click **Properties** to display the **Local Area Connection Properties** dialog box.
3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties** to display the **Internet Protocol (TCP/IP) Properties** dialog box.

5. On the General tab, select **Use the following IP address**. Enter the following:
   - IP address: `192.11.13.5`
   - Subnet mask: `255.255.255.252`

   Make a note of any IP addresses or other entries that you have to clear. You may need to restore them later to connect to another network.
6. Select **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
7. Click **Advanced** at the bottom of the dialog box to display the Advanced TCP/IP Settings dialog box.
8. Click the **DNS** tab. Make sure no DNS server is administered (the address field should be blank).
9. Click **OK**, **OK**, and **Close** to close all the windows.

Browser settings

Connecting directly to the media server

These steps change the browser settings.

Note:
Instructions are for Internet Explorer 6.0 only.

1. Click **Tools > Internet Options**.
2. Select the **Connection** tab.
3. In the LAN Settings box (lower righthand), click Advanced
4. In the Exceptions box after the last entry, type**: 192.11.13.6**
5. Click **OK**, then **OK**, then **OK** again to close all the dialog boxes.

Connecting remotely through the network

When connected through a proxy server, a connection session to a media server tends to time out. To avoid having the media server time out during a session, add the media servers' host names or IP addresses to the list of host names and IP addresses.

Note:

Instructions are for Internet Explorer 6.0 only.

1. Click **Tools > Internet Options**.
2. Select the **Connection** tab.
3. Click on **LAN settings**, then **Advanced**.
4. In the `Do not use proxy server for addresses beginning with`: field, type in the IP address for each media server you intend to access remotely. If the IP addresses have the first or first and second octets the same, you can shorten it to xxx.xxx.* (example, 135.9.*).
5. Click **OK**, then **OK**, then **OK** to close all the dialog boxes.

Appendix B: Troubleshooting an installation

This section provides some simple strategies for troubleshooting an installation of a media server. It focuses on possible problems when

Installing the media server hardware

The media server hardware includes the

- Media server(s)
- Ethernet switch
- Uninterruptible power supply (UPS)
- TN2312BP IP Server Interface circuit pack

Problem	Solution
No power to the UPS	- Make sure the UPS is plugged into the outlet. - Make sure the outlet has power. - See the user's guide that comes with UPS for other solutions.
No power to the Ethernet switch	- Make sure the Ethernet switch is plugged into the UPS or outlet. - Make sure the UPS or outlet has power. - See the user's guide that comes with the Ethernet switch for other solutions.
No power to the media server	- Make sure the media server is plugged into the UPS. - Make sure the UPS has power. - Push the power button on the front of the media server.
IPSI LEDs flash	- Make sure it is in the correct slot: (slot 1 for G650 Media Gateway, slot 2 for G600 Media Gateway, Tone-Clock slot for all others). - Ping IPSI from server. - Ping server from IPSI (it is connected to the top Services port on the IPSI).

Configuring the media server hardware

Problem	Solution
Cannot log into UPS subagent	- Make sure the SNMP Subagent is installed in the UPS. - Make sure you are connected to the correct Ethernet port. - Make sure you have the correct login ID and password. See the user's guide that comes with the SNMP Subagent. - Make sure the network card on the laptop is configured correctly.
Cannot log into Ethernet switch	- Make sure you are connected to the correct Ethernet port. (One Ethernet switch, it is the port marked Console) - Make sure you have the correct login ID and password. See the user's guide that comes with the Ethernet switch. - Make sure the network card on the laptop is configured correctly.
Cannot log into media server	- Make sure you are connected to the Services Ethernet port. (Default is port 2 [Eth1] on the back of the server). - Make sure you are using a crossconnect cable between the laptop and server. - Make sure the ARP cache is cleared on the laptop. In an MS-DOS window, type **`arp -d 192.11.13.6`** and press **Enter**. - Make sure you have connectivity. In an MS-DOS window, type **`ping 192.11.13.6`** and type **Enter**. - Make sure the NIC on the laptop is configured correctly.
Cannot access Avaya Installation Wizard	- Make sure you are plugged into the Services port (2 [Eth1]) - Make sure you are using the correct IP address: 192.11.13.6 - Make sure you are using the correct login and password. - Make sure the NIC on the laptop is configured correctly.
Cannot use SAT commands	- Make sure you are using the correct IP address: 192.11.13.6 and port 5023 - Make sure you are using the correct login and password.
Cannot ping out to customer's network	- Make sure that in the LAN security settings that "output from server" for icmp is enabled.
Cannot ping media server from customer's network	- Make sure that in the LAN security settings that "input to server" for icmp is enabled.

Problem	Solution
Cannot access media server remotely	- Make sure in the LAN security settings that "input to server" are checked for telnet (Linux commands), https (Web access), and def-sat (SAT commands access). The LAN security settings can be changed on the Web interface with a direct connection to the media server.
LED display on IPSI is flashing	- IPSI LED has not been programmed with switch and location (DHCP) - IPSI LED has not had an IP address assigned to it (static IP addressing)
Cannot access IPSI for static addressing	- Make sure you are plugged into the Services (top) port on the IPSI. - Make sure the ARP cache is cleared on the laptop. In an MS-DOS command window, type **`arp -d 192.11.13.6`** and press **Enter**.
No "V" on IPSI LED	- IPSI is not connected to Ethernet switch or network. Connect cable to bottom port on IPSI faceplate and to the Ethernet switch or the customer's network. - Make sure port on Ethernet switch assigned to that IPSI is enabled.
"V" on IPSI LED is not filled in	- IPSI does not have an IP address assigned to it. - IPSI has not been administered.
Get alarm when first connect to IPSI	- IPSI does not have current firmware. Upgrade firmware.

Installing the license and Avaya authentication files

Problem	Solution
Cannot get files from RFA site	- Provide the correct SAP number. - Provide the serial number for the reference IPSI
License file will not install	- Make sure there are not two license files on the server. If so, delete one of them. - May have corrupt file. Download file again from RFA site. - Upload using binary mode.
Media server is in no license mode	- Normal situation when license file is first installed because it cannot see the IPSIs; they do not have IP addresses yet. - After 30 minutes, license has not located reference IPSI. In a SAT session, type **`reset system 1`** and press **Enter** to reset the 30-minute clock.
Cannot use administration commands	- May be in No License Mode because 30-minute timer has lapsed. In a SAT session, type **`reset system 1`** and press **Enter** to reset the 30-minute clock.
ASG does not work	- Re-install Avaya authentication files.

Index

F

H

I

L

M

N

P

R

S

T

U

V