AVAYA

Installing and Configuring the Avaya S8700 or S8710 Media Server

03-300145
Issue 1
June 2004

Copyright 2004, Avaya Inc.
All Rights Reserved

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

Disclaimer

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:
- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. 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 Customer Equipment, ACA Technical Standard (TS) 001 - 1997.

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 and EN55022:1998.

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

Contents

Installing and Configuring the Avaya S8700 or S8710 Media Server 　**7**
June 2004

Contents

About This Documentation

This documentation, *Installing and Configuring the Avaya S8700 or S8710 Media Server* (03-300145), provides procedures for installing Avaya Communication Manager on and configuring an S8700 or S8710 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 S8700 or S8710 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 25.

Read the Pre-installation information on page 16 first. This section lists all the 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 Table 2, Avaya S8710 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 S8700 or S8710 Media Server (*555-245-703). 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 28
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) on page 31
- Configuring the media server on page 33
- Configuring second media server on page 41
- Translating the IPSIs on page 43

To complete the installation, you 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 <u>Connecting to the IPSIs</u> on page 49.

Complete the installation using information in the following sections:

- <u>Completing the installation administration</u> on page 57
- <u>Testing the media server installation</u> on page 69
- <u>Accessing the media server</u> on page 81

If problems occur during the installation, use <u>Troubleshooting an installation</u> on page 89 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 Avaya Communication Manager and refer to the most current documentation.

Physical dimensions

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

Terminology

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. It is the same as a port network. It can also refer to the MCC1 (multi-carrier cabinet).
- *UUCSS* refers to a circuit pack address in cabinet-carrier-slot order.

Typography

This section describes the typographical conventions for commands, keys, user input, system output, and field names.

Commands

Commands are in **bold sans serif** type.

Example

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

Command variables are in **bold sans serif *italic*** type.

Example

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

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

Example

Type **copybcf [-F34]**.

Keys

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

Example

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

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

Example

Press **ALT+D**.

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

Example

Press **Escape J**.

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

Example

Press **F3** (Save).

User input

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

Examples

- Type **exit**, and then press **Enter**.
- On the **File** menu, click **Save**.
- On the Network Gateway page, click **Configure** > **Hardware**.

Installing and Configuring the Avaya S8700 or S8710 Media Server   **11**
June 2004

System output and field names

System output on the screen is in monospaced type.

Example

- The system displays the following message:

      The installation is in progress.

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

Example

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

Downloading this book and updates from the Web

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

Avaya makes 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 can also 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 documentation uses the following safety labels and security alert labels:

⚠ CAUTION:

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

⚠ WARNING:

A warning statement calls attention to a situation that can result in harm to hardware or equipment, including ESD damage to electronic components.

⚠ DANGER:

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

⚠ SECURITY ALERT:

A security alert calls attention to a situation that can increase the potential for unauthorized access to a media server or use of a telecommunications system.

Related resources

For providing physical installation and connection information, see *Quick Start for Hardware Installation: Avaya S8700 or S8710 Media Server* (555-245-703).

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

For all documents associated with the S8700 or S8710 Media Server, including those described above, see *Documentation for Avaya Communication Manaager, Media Gateways and Servers* CD (03-300151).

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya Helpline 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. 120 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 S8700 or S8710 Media Server* (03-300145).

1 Introduction

These procedures are for installing Avaya Communication Manager and configuring a new Avaya S8700 or S8710 Media Server and associated components in either a Multi-Connect or an IP-Connect configuration. The installation procedures for both models are basically the same; where they differ is noted.

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 servers.

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

The following information is included in this installation procedure:

Pre-installation information

Before you go on site

Before going on site, make sure the customer has 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.

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 81 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

  — 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 (patch), if required, and license and Avaya authentication files on your services laptop.

- Verify that you have the current firmware available. 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 S8700 or S8710 Media Servers 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 the Remote Feature Activation (RFA) to obtain the license and Avaya authentication files. RFA is a Web-based application, available to Avaya employees and authorized Business Partners, that enables you to create and deploy license files for all 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 take the RFA online training and pass the online test.

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
- Serial number of one TN2312BP Internet Protocol Server Interface (IPSI) circuit pack designated the reference IPSI.
- Intranet 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 require 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 laptop. This includes, the filled-out *Electronic Preinstallation Worksheet* (EPW); any software updates; current firmware, and ART script.

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 (patch), 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 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

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-inch (48-centimeter) equipment racks are properly installed and solidly secured. Make sure that the screws that come with the racks are there. The S8700 Media Server requires a 2-post rack. The S8710 Media Server requires a 4-post rack. If using a rack cabinet, make sure it has adequate ventilation.

- Verify that the rail kit to support the S8710 Media Server are available for installation.

- Verify that the rail kits, required to support the very heavy UPSs, are installed on the rack or available for installation. For information on installing the rails, refer to the documentation that comes with the rail kits.

- 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 Internet Protocol Server Interface (IPSI) circuit packs is labeled and run from the control hardware rack to the port networks or that appropriate connectivity is provided.

- Verify that you have all the equipment on site. See Table 3, List of required hardware, on page 20 for the list of required hardware.

Equipment specifications

The media server control network components consist of two media servers, one or two Ethernet switch(es), and two UPSs. See Table 1, Control network components specifications, on page 18.

Table 1: Control network components specifications

Component	Dimensions English (in.)	Metric (cm)	Us (height in rack)	Weight (lb/kg)
Media Server				
S8700	3.5h x 17d x 17w	9h x 43d x 43w	2	25/11
S8710	3.4h x 26d x 17.5w	8.6h x 66d x 45w	2	60/27
Ethernet Switch:				
P133G2/P134G2	3.5h x 14d x 19w	9h x 35d x 48w	2	11,13/5,6
P333T/334T	3.5h x 18d x 19w	9h x 45d x 48w	2	16.5/7.5
UPS:				
700 VA	3.5h x 19d x 17w	9h x 48d x 43w	2	34/15
1500 VA	3.5h x 24d x 17w	9h x 30d x 43w	2	50/23

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

Table 2, Avaya S8710 Media Server features and specifications, on page 19 outlines the features and specifications of the Avaya S8710 Media Server.

> **NOTE:**
> Some values are shown at maximum configuration. Avaya values are slightly lower then the maximum.

Table 2: Avaya S8710 Media Server features and specifications *1 of 2*

Feature	Description
Microprocessor	1 Pentium 4
Memory	512 MB
Drives (SCSI)	Hard drive: 72 GB, 10K RPM
	CD/DVD-ROM: 24x maximum
	Floppy disk drive: 1.44 MB (3.5 in. [xx cm])
Physical Dimensions	Height: 3.4 in. [8.6 cm], 2 Us)
	Depth: 26-in. (66 cm)
	Width: 17.5-in. (45 cm)
	Maximum weight: 60 lb (27 kg)
Integrated Functions	2 10/100/1000BaseT Ethernet connectors
	Serial connector
	iLO connector (unused)
	Keyboard connector
	Mouse connector
	3 USB connectors
	Video connector
	VHDCI SCSI connector
Environment: Air Temperature	Ambient operating: 50° to 95° F (10° to 35° C)
	Maximum wet bulb: 82.4° F (28° C
	NOTE: All temperature ratings shown are for sea level. An altitude derating of 1.8° F per 1000 ft to 10,000 ft (1° C per 300 m) is applicable. No direct sunlight allowed.

Table 2: Avaya S8710 Media Server features and specifications *2 of 2*

Feature	Description
Environment: Humidity	Operating: 10% to 90%
	Nonoperating: 5% to 85%
	NOTE: Storage maximum humidity of 95% is based on a maximum temperature of 113° F (45 °C). Altitude maximum for storage corresponds to a pressure minimum of 70 KPa.
Electrical Input	Rated input voltage: 100 to 240 VAC
	Rated input frequency: 50 to 60 Hz
	Rated input current: 6 A (110 V) to 3 A (220 V)
	Rated input power: 600 W
	BTUs per hour: 2050
Power supply output	Rated steady-state power: 400 W
	Maximum peak power: 400 W

Required hardware

Before beginning the process, make sure you have the hardware listed in on hand.

Table 3: List of required hardware *1 of 2*

Comcode	Description	Number	Included	Optional	FRU
700293673 700326416	Avaya S8700 Media Server Avaya S8710 Media Server	2 2	Yes Yes		Yes Yes
408357002 408427409 700181928	Powerware 9125 uninterruptible power supply (UPS) (if Avaya-provided) – US & Canada – International – Japan	2		Yes (can be customer provided)	Yes
408427656	SNMP Network Interface Adapter for UPS (if Avaya-provided)	2		Yes	Yes
700230733 700230741	Rail kits for mounting UPSs in rack – 2-post rack (Powerware code: 05141562-0021) – 4-post rack (Powerware code: 05146726-5501)	2		Yes	Yes
108873233 108563123 108644451	10/100BaseT Ethernet switch (if Avaya-provided) – Avaya Ethernet P133 switch – Avaya Ethernet P333 switch – Avaya Ethernet P334 switch	1 or more		Yes	Yes
700169121	External V.90 56K USB modem with cable (if used)	2	Yes		Yes

Table 3: List of required hardware *2 of 2*

Comcode	Description	Number	Included	Optional	FRU
700181050	Formatted 128-MB PCMCIA PCCARD flashdisk (S8700 only)	2	Yes		Yes
700290448	Compact 4-slot flash drive (S8710 only)	2		Yes	Yes
700290430	128-MB compact flash media (S8710 only)	2	Yes		Yes
700287964	Avaya Communication Manager CD for Linux Servers	1	Yes		Yes
700335797	Documentation for Avaya Communication Manager, Media Gateways and Servers CD (03-300151)	1	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
700170004 700178072 700178122	Red CAT5 Ethernet cables (if duplicated control network) – 5-meter (16 feet) – 25-meter (82 feet) – 50-meter (164 feet)	4 2-68 2-68	Yes		Yes
700169998	Blue CAT5 Ethernet crossconnect cable for duplication	1	Yes		Yes
700179898 700252828	Yellow single-mode fiber optic cable with SC connectors (S8700 only) Yellow single-mode fiber optic cable with LC connectors (S8710 only)	1 1	Yes		Yes
700170053	Black CAT5 Ethernet crossconnect cable for laptop computer	1	Yes		Yes
407063478	Electrostatic discharge (ESD) wrist strap	1	Yes		Yes

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 S8700 or S8710 Media Server* (555-245-703)—a quick reference guide providing physical installation and connection information.

- Filled out *Electronic Preinstallation Worksheet (EPW)*—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 S8700 or S8710 Media Server* (03-300145)—this document, providing information on configuring the control network components, testing, and troubleshooting.

- The following job aids are also available on the *Documentation for Avaya Communication Manager, Media Gateways and Servers* CD (03-300151):

  - *Job Aid: Approved Grounds* (555-245-772)—job aid providing acceptable methods of grounding equipment.

  - *Job Aid: Server and CSS Separation—Avaya S8700 or S8710 Media Server* (555-245-766)—job aid providing information on and connectivity diagrams when the duplicated S8700 or S8710 Media Servers are in separate locations.

- *Upgrading Software and Firmware—Avaya S8700 or S8710 Media Server* (555-245-115)—part of the library providing information on upgrading Avaya Communication Manager and the firmware on 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 2.1, Media Gateways and Servers* (03-300190)—provides information on how to troubleshoot and replace various components.

- *Maintenance Commands for Avaya Communication Manager 2.1, Media Gateways and Servers* (03-300191)—provides information on how to use command interfaces, command syntax, and output from maintenance-related commands.

- *Maintenance Procedures for Avaya Communication Manager 2.1, Media Gateways and Servers (*03-300192)—provides information on how to use alarms, error codes, and tests to diagnose and repair problems.

Connecting to the customer's network

The media servers connect directly to the customer's network. The following section provides information on connecting the media server to the customer's network.

In a typical configuration, you connect to the network through a port on the back of the Avaya S8700 or S8710 Media Server, using a standard CAT5 cable with RJ45 connectors on each end. Typically, for an IP Connect configuration, you connect through port 1 (Eth0). For a Multi-Connect configuration, you connect through port 5 (Eth4). See or , connected to back of S8710 Media Server.

The other end of the cable connects to an Ethernet switch (router), hub, or token ring.

Figure 1: CAT5 cable connected to a port on the back of the Avaya S8700 Media Server
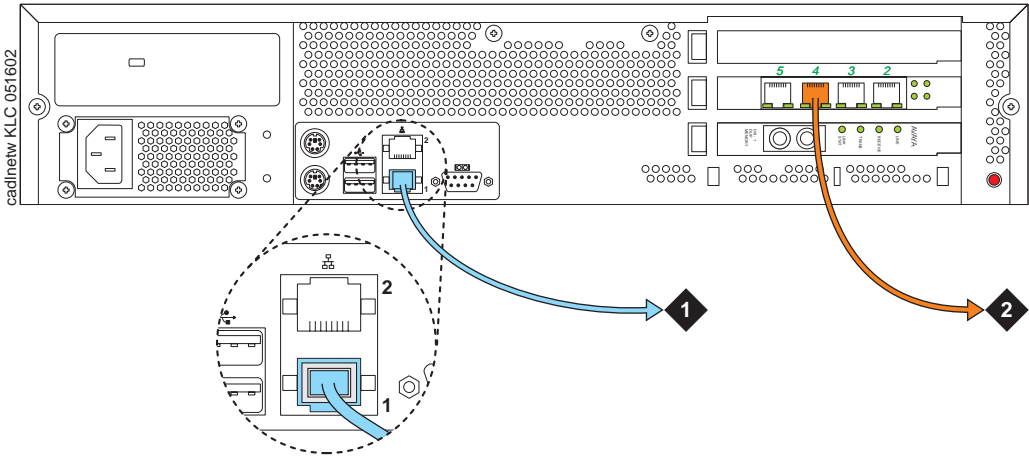

Figure notes

1   To network (nondedicated control network)

2   To network (dedicated control network)

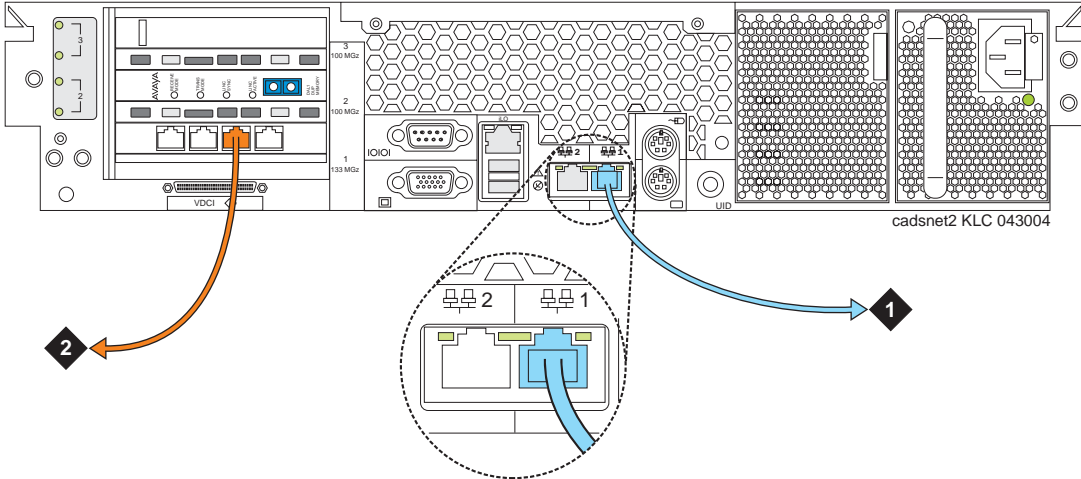**Figure 2: CAT5 cable connected to a port on the back of the Avaya S8710 Media Server**

Figure notes

1   To network (nondedicated control network)

2   To network (dedicated control network)

Installing and Configuring the Avaya S8700 or S8710 Media Server   **23**
June 2004

Connecting the USB modems

If you have not connected the modems yet, do so now.

> ⚠️ **WARNING:**
>
> Once you cable the modems to the media servers, do not unplug the modem USB cable on the *active* server. If the modem must be replaced, replace it when the media server is in standby mode.

> **NOTE:**
>
> USB and serial modems cannot connect to rotary lines. A Touch Tone line is required.

When you configure the media server, you set the modem options. No options are set on the modems themselves.

Connecting to collocated servers

Both servers share one telephone line. To connect to collocated servers:

1   Install two RJ11 jack outlets wired to a single 1MB (Measured Business) telephone line.

2   Connect the RJ11 jacks, one to each media server, using the modular telephone cord supplied with the modem.

3   Connect one modem, using the USB cable supplied with the modem, to media server 1.

4   Connect the other modem, using the USB cable, to media server 2.

Connecting to separated servers

Each server has a dedicated telephone line. To connect to separated servers:

1   Install one RJ11 jack outlet wired to a single 1MB telephone line for a media server in each location.

2   Connect the RJ11 jack to each media server, using the modular telephone cord supplied with the modem.

3   Connect each modem, using the USB cable, to the media server at each location.

> **NOTE:**
>
> For more information on media servers in two locations, see *Job Aid: Server and CSS Separation—Avaya S8700 or S8710 Media Server* (555-245-766).

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 S8700 or S8710 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.

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 servers are 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.

2 Configuring the hardware in the rack

Once the control network equipment is installed and connected, you must configure the SNMP Modules in each UPS (if Avaya supplied), the SNMP Subagent in the Avaya Ethernet switch (if Avaya supplied), and the two media servers. The first two are to allow that equipment to send alarms (traps) to the media servers.

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

This section covers the following tasks:

- Configuring the SNMP modules in the UPS on page 28
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) on page 31
- Configuring the media server on page 33
- Configuring second media server on page 41

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.

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 S8700 or S8710 Media Server* (555-245-703). Make sure you are plugged into the correct port on the SNMP module.

The SNMP module in each UPS must be administered so it reports alarms to the appropriate 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 (1 for each UPS)
- Default gateway IP address (1 only)
- 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.

⚠️ **WARNING:**
It is critical that each UPS report SNMP traps to the media server it is powering. For example, media server 1 should be plugged into UPS 1, and UPS 1 **must** be configured to report SNMP traps to the media server 1 actual IP address (not the Active Server address). The same required relationship holds true for media server 2 and UPS 2. This is important because if the UPS detects loss of commercial power and/or depletion of battery resources, it will send a trap to allow the media server to lower the media server's state of health to cause an interchange. If the UPS sends the trap to the wrong server trap receiver address, that media server **will interchange to** the media server that is plugged into the failing UPS.

See Setting selected traps (alarming) on page 30 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.

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
    - For UPS1, the defaults are 198.152.254.239, 255.255.255.0.
    - For UPS2, the defaults are 198.152.255.239, 255.255.255.0.
- IP address of the trap receiver. (Do not use the Active Server IP address.)
    - For UPS1, this is the IP address of media server 1 (default is 198.152.254.200).
    - For UPS2, this is the IP address of media server 2 (default is 198.152.255.200).
- 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 1 SNMP module and the other end to the next available port on the Ethernet switch for Control Network A (CNA).

9   Depending on whether a single or duplicated control network is installed (Single control network on page 30 or Duplicated control network on page 30), repeat steps 5 thru 7 for the UPS 2 SNMP module.

10 Connect one end of a CAT5 cable to the RJ45 connector on the UPS 2 SNMP module and the other end to the next available port on the Ethernet switch for Control Network A (CNA).

Single control network

If a single control network, use the following address and cable connection information for UPS 2:

- UPS IP address / Subnet mask = **198.152.255.238 / 255.255.255.0**
- Default Gateway IP address = **198.152.254.202**
- Host Table trap receiver IP address = **198.152.254.202**
- Local network administrator supplied information as required for Get and Set community name strings.
- Cable the RJ45 connector on the UPS 2 SNMP module to the next available port on the Ethernet switch for Control Network A (CNA).

Duplicated control network

If a duplicated control network, use the following addresses and cable connection information for UPS 2:

- UPS IPaddress / Subnet mask = **198.152.255.239 / 255.255.255.0**
- Default Gateway IP address = **198.152.255.202**
- Host Table trap receiver IP address = **198.152.255.202**
- Local network administrator supplied information as required for Get and Set community name strings.
- Cable the RJ45 connector on the UPS 2 SNMP module to the next available port on the Ethernet switch for Control Network B (CNB).

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:**
> We do not know which Avaya Ethernet switch model or firmware load the factory is shipping. Therefore, we cannot provide specific instructions in this document on how to configure the SNMP subagent. Refer to the documentation that comes with the switch.

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 (1 for each Ethernet switch)
- Subnet mask
- Trap receiver IP address
- Community string (get, set, trap)
    - Spanning tree
    - 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.
   - For a single control network—connect Ethernet switch 1 for Control Network A (CNA) into UPS 1.
   - For a duplicated control network—connect Ethernet switch 1 for CNA into UPS 1 and connect Ethernet switch 2 for Control Network B (CNB) into UPS 2.
2. Connect the services laptop computer (RS-232 serial port) to the port labeled Console on the front of Ethernet switch 1 (CNA) 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(es)

 — For Ethernet switch for CNA, the defaults are 198.152.254.240, 255.255.0.0.

 — For Ethernet switch for CNB, the defaults are 198.152.255.240, 255.255.0.0.

- IP address of the trap receiver. (Do not use the Active Server IP address.)

 — For Ethernet switch for CNA, this is the IP address of media server 1. (default is 198.152.254.200)

 — For Ethernet switch for CNB, this is the IP address of media server 2. (default is 198.152.255.200)

- SNMP community string for Get, Set, and Trap. (See the section on SNMP commands on the documentation CD that comes with the Avaya Ethernet switch.)

⚠ SECURITY ALERT:

The **Get** and **Set**, community name strings are generally configured with default values of **Public** and **Private,** respectively. These community name strings function as passwords for their respective SNMP operation. 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　Set spanning-tree to disabled (default is enabled)

 Use the command **set spanning disable**.

8　If IP Connect, make sure all appropriate ports on the Ethernet switch are locked to 100 speed using full duplex.

9　When completed, disconnect the services laptop computer from the Ethernet switch.

10　If two Ethernet switches are present for CNA, repeat steps 1 through 7 for the second switch.

11　If a duplicated control network, repeat steps 1 through 9 for the remaining Ethernet switch(es).

Configuring the media server

A new media server comes with a blank hard drive and a bootable CD-ROM with Linux operating system and Release 2.1 of Avaya Communication Manager on it.

Use the instructions in *Quick Start for Hardware Installation: Avaya S8700 or S8710 Media Server* (555-245-703) to install the media servers in the data rack. After installing the media servers, you must install the software from the CD onto the hard drive of each media server.

This section covers the following tasks:

- Clearing the ARP cache on the laptop on page 33
- Powering up the media server on page 34
- Accessing the media server on page 34
- Setting up Telnet on page 34
- Installing Avaya Communication Manager on page 35
- Using the Installation Wizard on page 36
- Configuring the modem on page 39
- Testing the media server LEDs on page 40
- Disconnecting from the media server on page 40
- Configuring second media server on page 41

> **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 Appendix A, Network configuration on page 87.

Clearing the ARP cache on the laptop

> **NOTE:**
> 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

1 **S8700**: Connect the AC power cord to media server 1 and to UPS 1 to power it up.

S8710: Connect the AC power cord to media server 1 and to UPS 1. Press the Power button on the front to power it up.

Accessing the media server

> **NOTE:**
> You must place the CD in the drive immediately.

1 Connect the laptop to the services port (port 2 [Eth1]) on the back of the media server using a crossconnect cable.

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

3 Wait at least 3 minutes after powering up before starting a Telnet session to access the information on the CD.

Setting up Telnet

> **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

⚠️ **CAUTION:**

If after you open a Telnet session on the media server and you get a login prompt, you may have a hard drive with software on it rather than a blank hard drive. If that is the case, go to Remastering the hard drive on page 41, then come back to this step.

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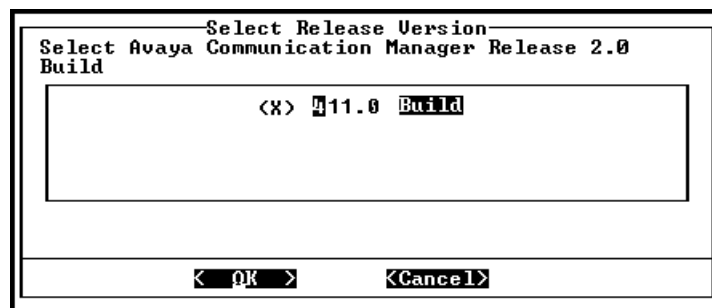
Use a telnet session to access the information on the CD.

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

```
┌─────────────────What do you want to do?─────────────────┐
│ The hard drive is currently Partitioned                 │
│  Choose One                                             │
│ ┌──────────────────────────────────────────────────────┐│
│ │    (X) Install    Install or Upgrade MV Software      ││
│ │    ( ) Shell      Boot to Rescue Bash Shell           ││
│ │    ( ) Quit       Reboot the server                   ││
│ │                                                        ││
│ │                                                        ││
│ └──────────────────────────────────────────────────────┘│
│                                                          │
│                      ‹   OK   ›                          │
└──────────────────────────────────────────────────────────┘
```

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 Select **<Yes>** and press **Enter**.

```
┌──────────────Select Release Version──────────────┐
│ Select Avaya Communication Manager Release 2.0    │
│ Build                                             │
│ ┌───────────────────────────────────────────────┐│
│ │            (X) 711.0 Build                     ││
│ │                                                ││
│ │                                                ││
│ └───────────────────────────────────────────────┘│
│                                                   │
│         ‹   OK   ›          ‹Cancel›              │
└───────────────────────────────────────────────────┘
```

4 Select **<OK>** and 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.

```
21:26:38 |  copying iputils-20020124-8.i386.rpm
21:26:38 |  copying libattr-2.0.8-3.i386.rpm
21:26:38 |  copying libcap-1.10-12.i386.rpm
21:26:39 |  copying libelf-0.8.2-2.i386.rpm
21:26:39 |  copying libgcc-3.2-7.i386.rpm
21:26:39 |  copying libjpeg-6b-21.i386.rpm
21:26:39 |  copying libtermcap-2.0.8-31.i386.rpm
21:26:39 |  copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 |  copying losetup-2.11r-10.i386.rpm
21:26:39 |  copying lrzsz-0.12.20-14.i386.rpm
21:26:39 |  copying lsof-4.63-2.i386.rpm
21:26:39 |  copying ltrace-0.3.10-12.i386.rpm
21:26:39 |  copying mailx-8.1.1-26.i386.rpm
21:26:39 |  copying mingetty-1.00-3.i386.rpm
21:26:39 |  copying mktemp-1.5-16.i386.rpm
21:26:39 |  copying ncompress-4.2.4-31.i386.rpm
21:26:39 |  copying net-tools-1.60-7.i386.rpm
21:26:40 |  copying patch-2.5.4-14.i386.rpm
21:26:40 |  copying pcre-3.9-5.i386.rpm
21:26:40 |  copying popt-1.8-0.69AV1.i386.rpm
21:26:40 |  copying rdate-1.2-5.i386.rpm
21:26:40 |  copying rusers-0.17-21.i386.rpm
21:26:40 |  copying setserial-2.17-9.i386.rpm
```

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.

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 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.
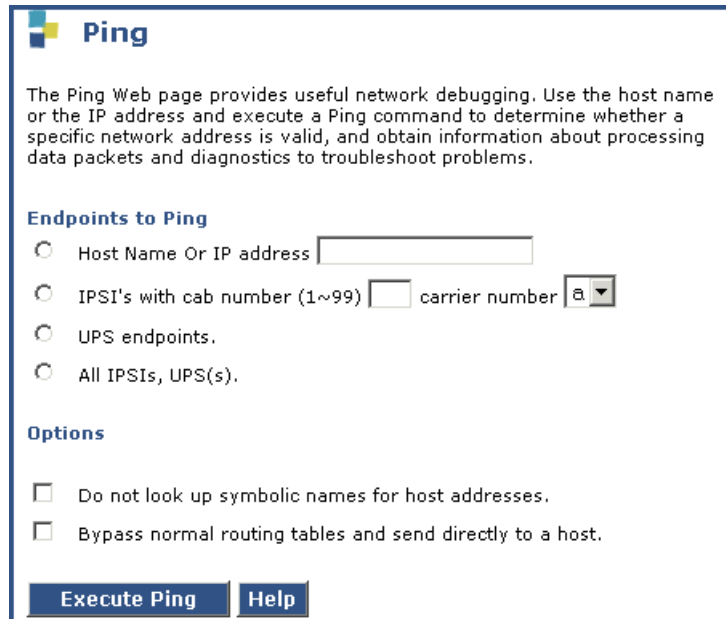
5 Click **Launch Avaya Installation Wizard**.

6 Follow the prompts, using Help on each page for more information.

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**.

Ping

The Ping Web page provides useful network debugging. Use the host name or the IP address and execute a Ping command to determine whether a specific network address is valid, and obtain information about processing data packets and diagnostics to troubleshoot problems.

Endpoints to Ping

○   Host Name Or IP address [   ]

○   IPSI's with cab number (1~99) [   ] carrier number [a ▼]

○   UPS endpoints.

○   All IPSIs, UPS(s).

Options

☐   Do not look up symbolic names for host addresses.

☐   Bypass normal routing tables and send directly to a host.

[Execute Ping]   [Help]

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.

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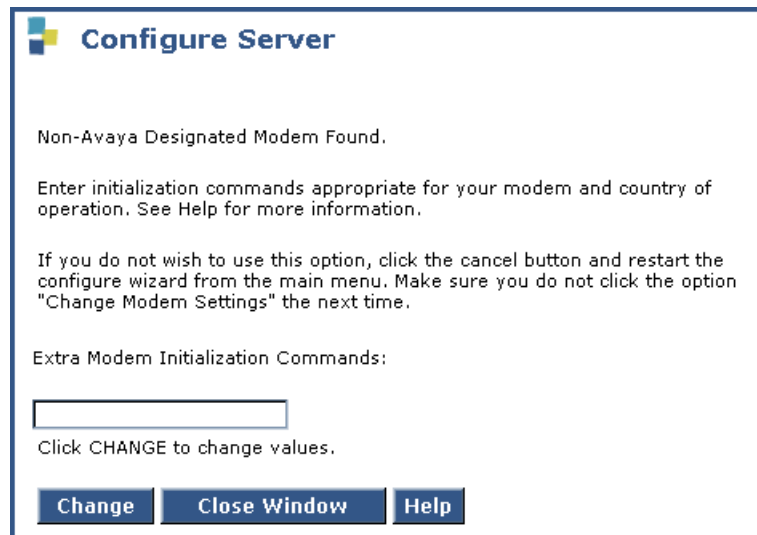
6 In the **AT String** field, type the initialization commands appropriate for your modem and country of operation. Click Help for guidance on what to enter.

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**.

Testing the media server LEDs

1 Under **Diagnostics**, click **Test Server LEDs** to test the media server LEDs.

2 Observe the Active/Standby and U2 LEDs on the front of the media server and the transmit LED on the duplication card on the back of the media server to ensure they are blinking. The blinking stops after about a minute.

1

Disconnecting from the media server

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

Configuring second media server

The procedures for this installation are the same as for configuring the first media server. Repeat tasks Clearing the ARP cache on the laptop on page 33 through Disconnecting from the media server on page 40 for the second media server.

Remastering the hard drive

> ⚠️ **CAUTION:**
> This task is not part of the ordinary configuration process and erases any information on the drive. Do not perform this task unless you are updating from a release prior to Release 2.1 of Avaya Communication Manager.

> **NOTE:**
> This step upgrades the server, loading the RP software onto the backup partition. The currently running release remains on the other partition, just as it always does during an upgrade.

1 Insert the CD containing the software into the CD-ROM drive on the media server and close the tray.

2 Under Server Configuration and Upgrades, click **Install New Software Release**.

3 Select from the menu the file from the CD (S8700-00.0-0000.0). Click **Continue** to complete the software installation.

On the page asking about installing the license file, select either statement and click **Continue**. The license file is replaced later in the upgrade process.

On the page asking about installing the Avaya authentication files, select **Do not update authentication information** and click **Continue**.

4 Select **Reboot** when you get to that Web page.

After the system reboots, which takes about 3 minutes, the RP software redirects the system to boot from the CD-ROM drive. This is the same software that would have loaded if the CD were bootable. Note that no telephony support is provided by this software. Its only purpose is to reformat the hard drive and install a clean copy of the Avaya Communication Manager server software.

5 Close the browser.

3 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 1.11 or a later version of Avaya Site Administration, to administer new features in Release 2.1 of Avaya Communication Manager.

> **NOTE:**
> For SAT commands you must be on the *active* media server.

Perform these tasks to customize the media server:

- Starting terminal emulation on page 43
- Inputing translations on page 44
- Resetting the media server on page 44
- Adding media gateways on page 44
- Administering the IPSIs on page 45

Starting terminal emulation

> **NOTE:**
> Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are supported terminal emulation applications.

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**.

Inputing translations

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

1 Type **save translations** 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.

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.

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

NOTE:
This procedure enables the IPSI circuit packs and allows 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: vodka
        Primary Control Subnet Address: 198.152.254.  0 *
      Secondary Control Subnet Address: 198.152.255.  0 *

OPTIONS

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

2 Verify that the Primary and Secondary Subnet Addresses are correct.

The subnet addresses must match the most significant 3 octets (the first three 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 the software with the correct subnet information.

> **⚠ CAUTION:**
> If the information displayed in the **Primary Control Subnet Address** and/or **Secondary Control Subnet Address** fields is not correct, it must be changed on the media servers. 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 thru 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

NOTE:
The information you provide differs, depending on whether the IPSIs get static addresses or they are assigned automatically through DHCP.

1   Type **add ipserver-interface** *PNnumber* and press **Enter** to add the IPSI circuit pack information.

2   When using a DHCP server, verify that the fields associated with the Primary IPSI and Secondary IPSI (if equipped) are populated with default data.The `Host:` and `DHCP ID:` fields are set by the DHCP server.

```
add ipserver-interface 4                                    Page   1 of   1
          IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 4

IP Control? y                                    Socket Encryption? n

                                                        Enable QoS? n


 Primary IPSI
 ------------
  Location:  9A01
      Host: ipsi-A09a
   DHCP ID: ipsi-A09a


 Secondary IPSI
 --------------
  Location:  9B01
      Host: ipsi-A09b
   DHCP ID: ipsi-A09b
```

When using 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.

Enabling IPSI duplication (duplicated control network only)

Enabling IPSI duplication requires that all IPSI-connected port networks have both primary (CNA) and secondary (CNB) IPSI circuit packs. Disabling IPSI duplication requires that all primary IPSI circuit packs be active.

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

S8700/S8710 MC:

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




        Enable Operation of PNC Duplication? y

      Enable Operation of IPSI Duplication? y

```

S8700/S8710 IP:

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




      Enable Operation of IPSI Duplication? n

```

2   Set the **Enable Operation of IPSI Duplication?** field to **y**.

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

Setting 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

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

4 Connecting to the IPSIs

> **NOTE:**
> The media gateways must be installed, connected to each other, and powered up.

This chapter covers the following tasks:

- [Programming the IPSI circuit packs](#) on page 50
  - [Using DHCP addressing](#) on page 50
  - [Using static addressing](#) on page 51
- [Verifying that IPSIs are translated](#) on page 54
- [Verifying connectivity to media server](#) on page 55
- [Upgrading IPSI firmware version (if necessary)](#) on page 55
- [Enabling control of IPSIs](#) on page 55
- [Verifying license status](#) on page 56
- [Reusing a TN2312AP/BP circuit pack](#) on page 56

> **NOTE:**
> At a minimum you must program the reference IPSI and connect to it to avoid going into No License Mode.

> **NOTE:**
> 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.

Single control network: Connect one end of the GREEN CAT5 straight-through cable to the IPSI adapter on the back of media gateway in position A.

Duplicated control network: In addition connect one end of the RED CAT5 straight-through cable to the IPSI adapter on the back of media gateway in position B.

Dedicated control network: The other end is connected to the next available port on the Ethernet switch.

Nondedicated control network: The other end is connected to the next available port on the customer's network.

For a connectivity guide, see *Quick Start for Hardware Installation: Avaya S8700 or S8710 Media Server* (555-245-703).

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.

> **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

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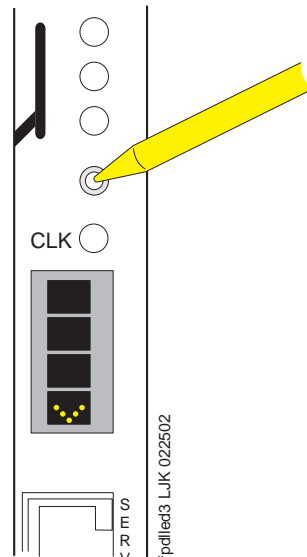
> **NOTE:**
> If you pass up the letter or number that you want, you must either cycle through all the letters or numbers to get to the one you want or reinsert (reseat) the circuit pack and begin again.

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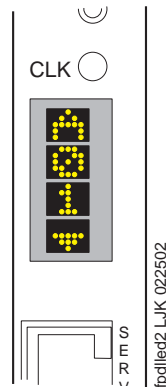
For duplicated control network, repeat these steps for the second IPSI in the cabinet.

Using static addressing

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 1: Connecting directly to the IPSI

cadlipsi KLC 031502
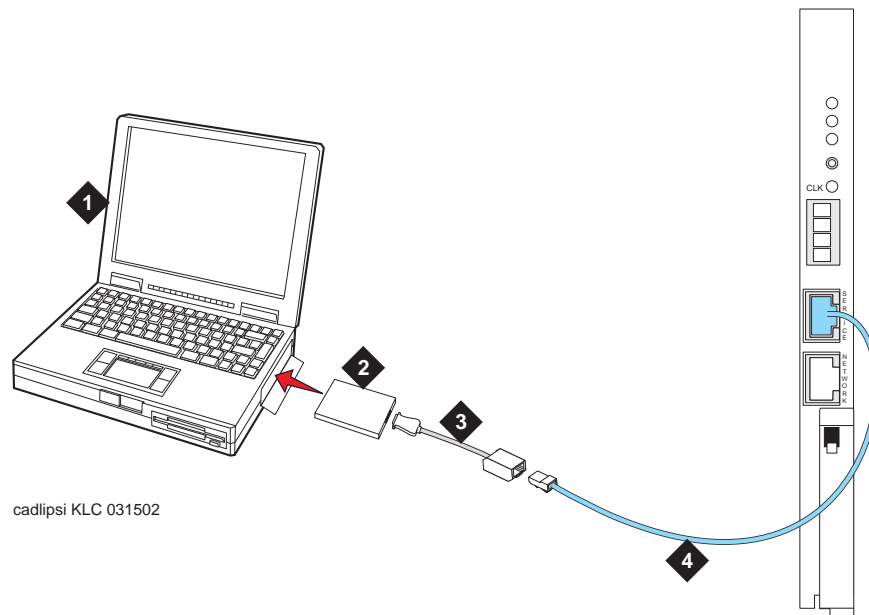
Figure notes

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

> **NOTE:**
> Make sure you have the password before proceeding.

1 Connect the services laptop computer to the top port on the IPSI circuit pack faceplate.

2 From the services laptop Start Menu, click **Start > Run** to open the Run dialog box.

3 Type **command** and press **Enter** to open a MS-DOS Command Line window.

4 Type **arp -d 192.11.13.6** and press **Enter** to clear the 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 contain an entry in the ARP cache.

5 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.

6   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.

7   Log in as **craft**.

Prompt = [IPADMIN]:

Type show control interface and press Enter.   **8**Type **show port 1** and press **Enter** to see the current settings.

9   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]: █
```

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

11   Type **show control interface** and press **Enter**.
The IP address, subnet mask, and default gateway information will be displayed.
Verify that the proper information was entered.

12   If required, type **set control gateway *gateway*** and press **Enter**, where ***gateway*** is the customer-provided IP address for their gateway.

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

14   If required, use the **set vlan priority**, **set vlan tag**, **set vlan id**, **set port negotiation** (1=disable), **set port duplex** (1 full), **set port speed** (1 100 MB), and **set diffserv** commands to enter VLAN and diffserv parameters for the IPSI. Use **Help** to obtain syntax guidelines for these commands.

15   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.

16 Type **quit** to logoff the IPSI.

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

17 Check the LCD. Verify that it has an I P with a filled-in V showing at the bottom. (See Figure 2, LED display showing that the IPSI has a static IP address, on page 54)

Figure 2: LED display showing that the IPSI has a static IP address
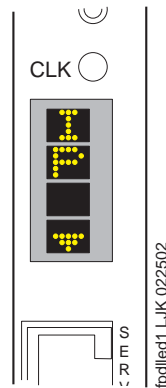
18 Disconnect the laptop from the faceplate.

> **NOTE:**
> Always use the **arp -d 192.11.13.6** command (step 4) to 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.

19 Repeat for each IPSI circuit pack.

Verifying that IPSIs are translated

> **NOTE:**
> You must be on the *active* media server to use SAT commands.

1 Type **list ipserver-interface** and press **Enter**.

2 Verify that all ISPI circuit packs are translated.

Verifying connectivity to 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.

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.

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 S8700 or S8710 Media Server* (555-245-115), Upgrading IPSI Firmware.

Enabling control of IPSIs

NOTE:
Make sure the IPSIs have the same, current firmware.

If a duplicated IPSIs, make sure that IPSI duplication is enabled before enabling IPSI control. See Enabling IPSI duplication (duplicated control network only) on page 47.

NOTE:
This procedure enables the IPSI circuit packs and allows 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

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

Reusing a TN2312AP/BP circuit pack

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 2.1, Media Gateways and Servers* (03-300192).

5 Completing the installation administration

This section covers the following tasks:

Verifying 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

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

NOTE:
You can only resolve alarms on the *active* media server.

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.

Enabling and disabling Ethernet switch ports

You may want to disable unused ports on the Avaya Ethernet switch (if used). To enable or disable Ethernet switch ports:

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

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

3   Locate the port(s) you want to disable and click on the button in the Disable column.

4   Click **Submit Changes**.

Backing up files to the compact flash media (S8710 only)

1   Connect the compact flash drive to one of the USB ports on the back 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.

Select **Save ACP translations prior to backup** to save translations to the media server's system disk before backing up the data.

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.

Backing up files to the PCMCIA flashcard (S8700 only)

1 Place the PCMCIA flashcard into the *bottom* slot of the PCMCIA drive in the active media server. See on page 63.

Figure 3: Placing the flashcard in the media server

h1dlopt LJK 030102
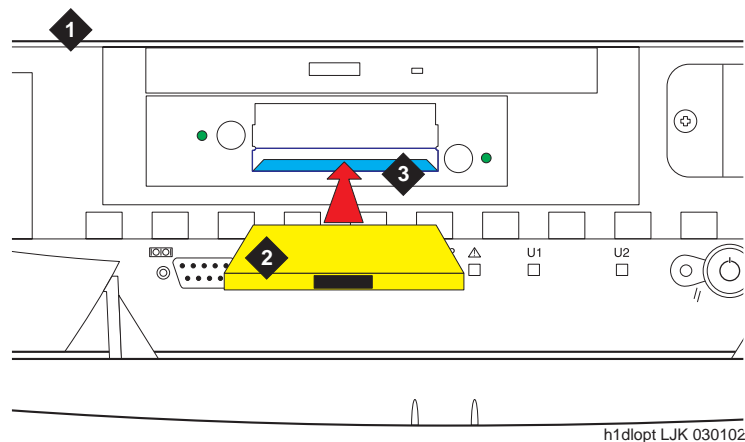
Figure notes

1	Media Server	**3**	Bottom slot of PCMCIA drive
2	PCMCIA flashcard		

2   Under Data Backup/Restore click **Backup Now**.

Backup Now

The Backup Now Web page lets you store data separate from the Avaya
media server. Select the type of data and the method to backup. Encrypting
the data while backing up provides you a high level of security and is
strongly encouraged.

Data Sets

☐ Avaya Call Processing (ACP) Translations
   ○ Save ACP translations prior to backup
   ○ Do NOT save ACP translations prior to backup
☐ Server and System Files
☐ Security Files

Backup Method

○ FTP

   User Name   [   ]
   Password   [   ]
   Host Name   [   ]
   Directory   [   ]

○ Email

   User Name   [   ]
   Domain Name   [   ]
   Mail Server   [   ]

   **Please Note: Depending on the size of the backup, the email may
   or may not work, as all mail servers have a maximum size they'll
   accept.

○ Local PC Card   Retain [   ] data sets at destination
          ☐ Format PC Card

Encryption

☐ Encrypt backup using pass phrase [   ]

[Start Backup]   [Help]

3   Select all applicable data sets.

Select **Save ACP translations prior to backup** to save translations to the media server's hard
drive before backing up the data.

4   Select Local PC card as the backup method.

   NOTE:
   Customer's may want to back up using another method.

5   Click **Backup now** to back up all data to the PCMCIA flashcard.

Telneting to media server

Enabling alarms uses Linux commands through Telnet.

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** (if business partner).

Enabling alarms

To INADS via modem

> **NOTE:**
> These steps must be done on both media servers.

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.

> **NOTE:**
> These steps must be done on both media servers.

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.

To INADS on second server

1   Connect to the second media server

2   Repeat <u>Telneting to media server</u> on page 65 through <u>Enabling alarms</u> on page 65 on the second server.

Installing and Configuring the Avaya S8700 or S8710 Media Server   **65**
June 2004

Registering the system

Follow the existing process and procedures to register the Avaya S8700 or S8710 Media Server.

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

6 Installing the media gateways

In a new installation, the Avaya S8700 or S8710 Media Servers work with only the Avaya G650 Media Gateway. However, an Avaya MCC1 Media Gateway is provided in a multiconnect configuration when a switch node carrier (SNC) for Center Stage Switch (CSS) is required. The MCC1 Media Gateway may contain one port network in the A, B, C, and D positions and the SNC in the E position. For duplicated bearer networks, the D position also may be used for the duplicated (B-PNC) SNC.

In a migration the media servers work with Avaya MCC1 and SCC1 Media Gateways in a multiconnect configuration, and G600 or CMC1 Media Gateways in an IP configuration.

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

Media gateways typically are installed in the same equipment room as the media server rack hardware (control network); however, they 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)
- *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)

7 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 71.

> **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 on page 69
- Testing the license file on page 70

> **NOTE:**
> Do these steps using a SAT session

> **NOTE:**
> For SAT commands you must be on the *active* media server.

Testing 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 4, Sample IPSI 01A test results screen—page 1, on page 70.

Figure 4: 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.

1 Type **test license [short | long]** and press **Enter**.

2 Verify the screen displays a *Test Results* screen similar to

Figure 5: 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 2.1, Media Gateways and Servers* (03-300190) 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:

- Major Alarms—Failures that cause critical degradation of service and require immediate attention.

- 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.

- 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 LEDs located on the media server.

More detailed information is available here for:

- S8700 Media Server LEDs on page 71
- S8710 Media Server LEDs on page 74
- Avaya Ethernet switch LEDs on page 76
- Uninterruptible power supply LEDs on page 77
- IPSI LEDs on page 77

S8700 Media Server LEDs

The media server has the LEDs shown in Figure 6, LEDs on front and back of S8700 Media Server, on page 72:

Figure 6: LEDs on front and back of S8700 Media Server

scdlled KLC 030502
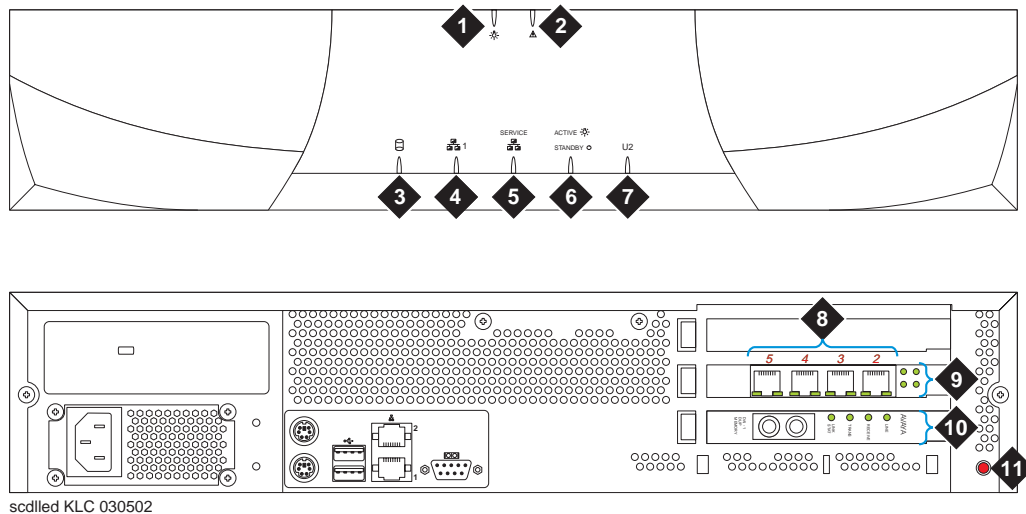
Figure notes

1	Power	**7**	U2 (not defined)
2	Configuration fault	**8**	4 NIC ports (the numbers indicate their assigned Ethernet ports)
3	Hard drive activity		
4	Network activity (CNA)	**9**	LEDs for the NIC ports (some NICs may not have LEDs)
5	Service—configuration health		
6	Active or standby mode indicator	**10**	LEDs for fiber optic duplication connectivity
		11	Status LED (not used)

Testing the media server LEDs

You can test some of the LEDs on the front of the media server through the Maintenance Web Interface. This makes sure that the Active/Standby and U2 LEDs (on the front of the media server) and the transmit LED on the DAJ1 duplication memory card (on the back of the media server) are controllable and not burned out and that the media server is not hung.

> **NOTE:**
> The U2 LED is controlled by the S8700 Media Server but does not have an assigned function.

The other LEDs are exclusively under hardware control so will not flash during the test. See the OEM user documentation that comes with the media server for information on those LEDs.

During the 1-minute test, the Active/Standby and U2 LEDs alternate from being on (amber) for 1 second and off for 1 second off. The transmit LED cycles from red (on 1 second, off 1 second) to green (on 1 second, off 1 second).

Using the Maintenance Web Interface, test the LEDs on the front of the media server:

1 Under Diagnostics, click **Test Server LEDs**.

2 On the Test Server LEDs screen, click **Test LEDs**.

3 Observe the Active/Standby and U2 LEDs on your media server and the transmit LED on your duplication card (back of media server) to ensure they are blinking.

Interpreting the test results

An abnormal condition is indicated if an LED shows any of the following flashing patterns.

- LED flashes **red**. This indicates that the green element is either burned out or not controlled.

- LED flashes **green**. This indicates that the red element is either burned out or not controlled.

- LED flashes between **red** and **amber**. This indicates that the red element is stuck on.

- LED flashes between **green** and **amber**. This indicates that the green element is stuck on.

- LED stays **amber** continuously. This indicates that either the media server is hung or the LED controller is stuck.

- LED stays **off** continuously. This indicates that the media server is hung or powered off, the controller is stuck, or the media server is using a new or different LED controller.

If the media server is hung, you do not need to do anything. It should automatically reboot and fix itself. If the media server does not reboot itself, power it down and then reboot it.

If an LED is clearly stuck or has a burned out element, ignore the indicators until you can conveniently replace the media server.

LEDs on the back of the media server

There are two sets of LEDs on the back of the media server: one set for the 4-port NIC card and one set for the fiber optic cable used for memory shadowing. The GREEN LEDs to the right of the NIC ports light up when they are in use. The GREEN LEDs to the right of the fiber optic cable indicate that the cables are connected correctly.

S8710 Media Server LEDs

The S8710 Media Server has the LEDs shown in Figure 7, LEDs on front panel of S8710 Media Server, on page 74 and Figure 8, LEDs on back panel of S8710 Media Server, on page 75.

Currently, there is no method to test the LEDs on the S8710 Media Server.

Figure 7: LEDs on front panel of S8710 Media Server

msdsled1 KLC 041304
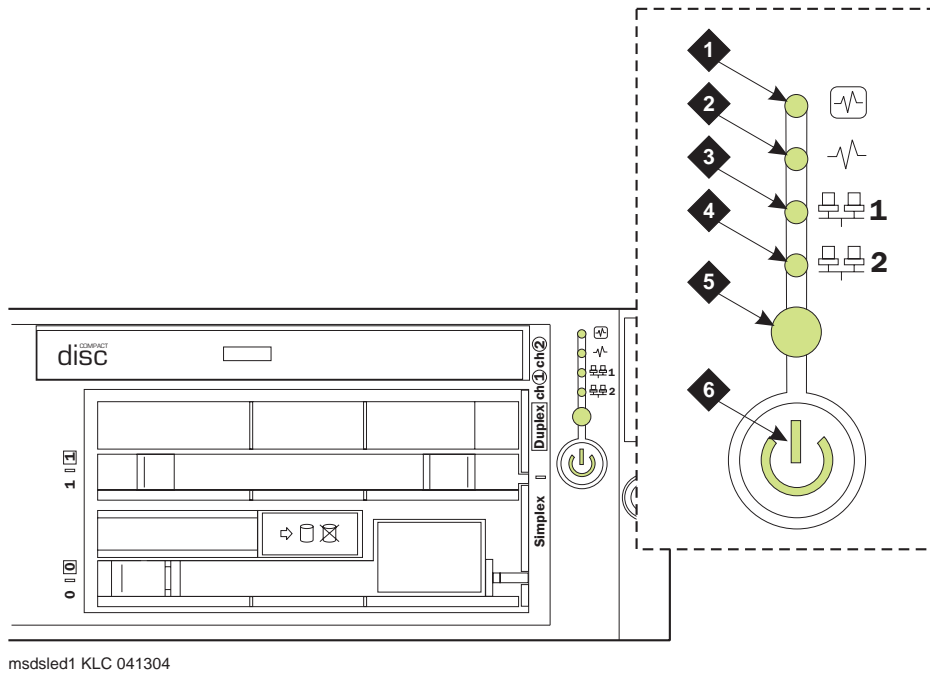
Figure notes

1	Internal health	**4**	NIC 2 (Eth1) link/activity (GREEN)
2	Power supply	**5**	Active/Standby mode (BLUE)
3	NIC 1 (Eth0) link/activity (GREEN)	**6**	Power on/standby button/system power

Figure 8: LEDs on back panel of S8710 Media Server
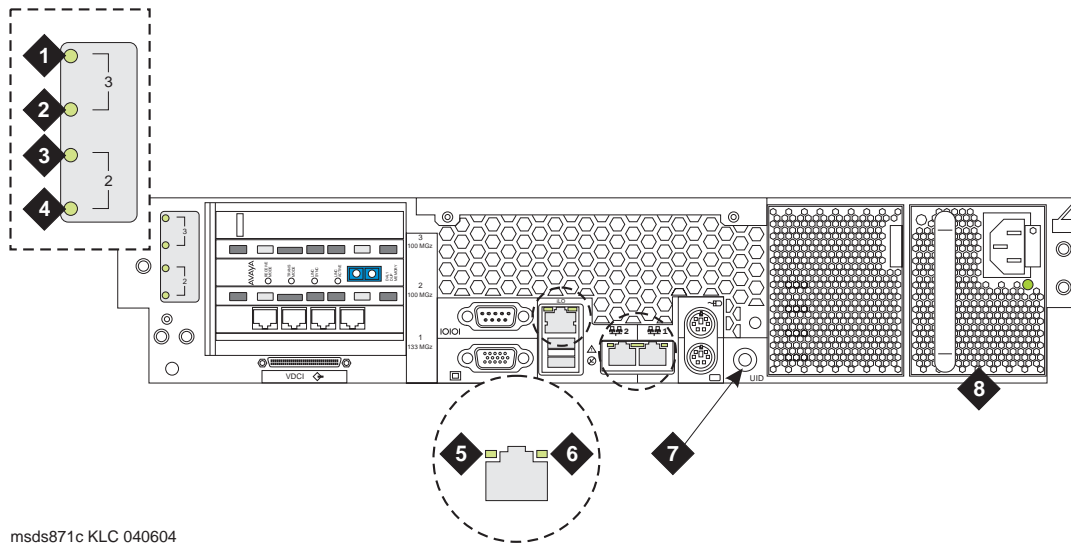
msds871c KLC 040604

Figure notes

1	Not used	**5**	RJ45 link (GREEN)
2	Not used	**6**	RJ45 link (GREEN)
3	DAL1 fault (AMBER)	**7**	Active/standby mode (BLUE)
4	DAL1 power (GREEN)	**8**	Power supply (GREEN)

Avaya Ethernet switch LEDs

The Avaya Ethernet Switch P333T has the LEDs shown in Figure 9, LEDs on Avaya P333T Ethernet switch, on page 76:

Figure 9: LEDs on Avaya P333T Ethernet switch
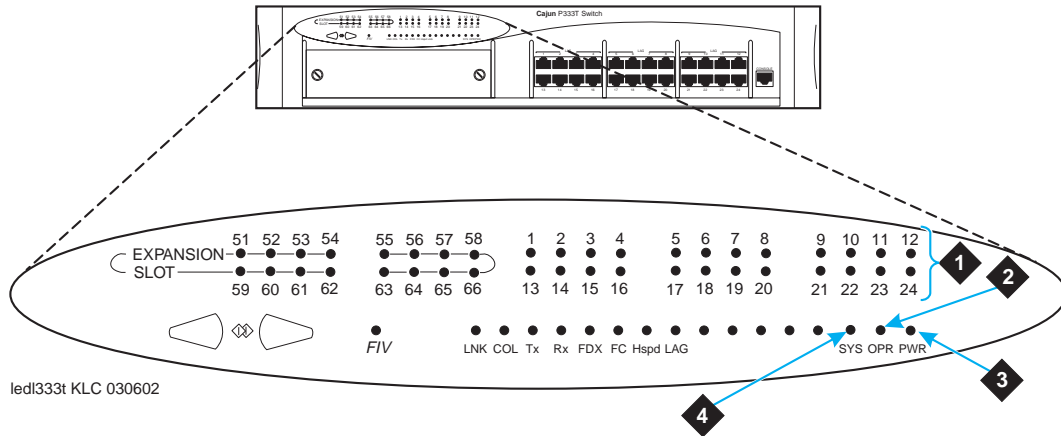
Figure notes

1	Ports in use	**3**	Power
2	CPU boot status	**4**	Lights if this module is the Avaya P33x stack master agent

For descriptions of the other LEDs, see the quick start guide and user guide that comes with the model of Avaya Ethernet switch you have.

Uninterruptible power supply LEDs

The Powerware uninterruptible power supply (UPS) front panel has the LEDs shown in Figure 10, LEDs on Powerware 9125 UPS, on page 77:

Figure 10: LEDs on Powerware 9125 UPS

ledIups KLC 030102
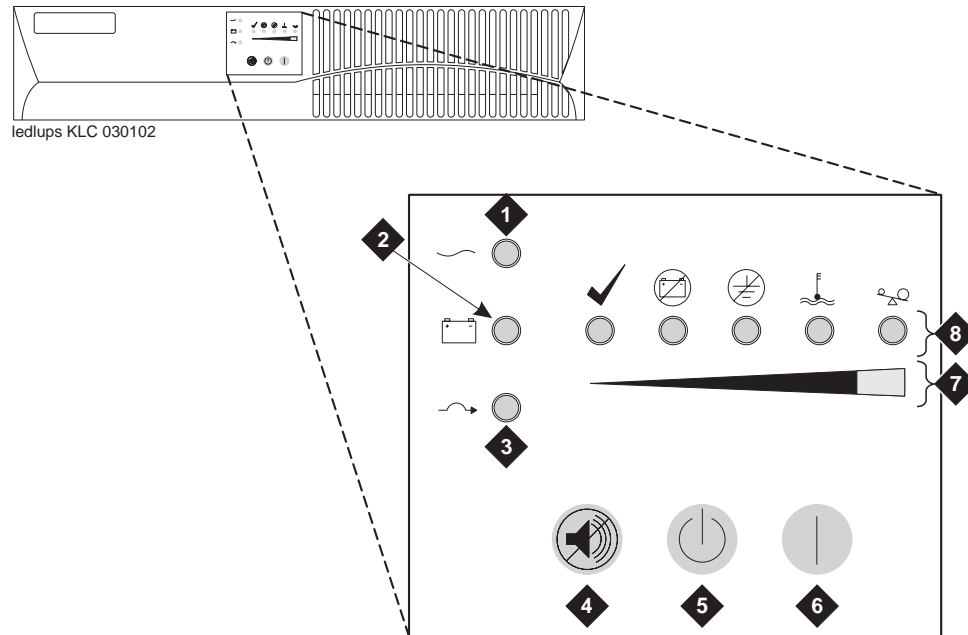
Figure notes

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

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 11, TN2312BP circuit pack faceplate, on page 78). 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 12, LED display on the IPSI circuit pack—static address, on page 79.

Figure 11: TN2312BP circuit pack faceplate
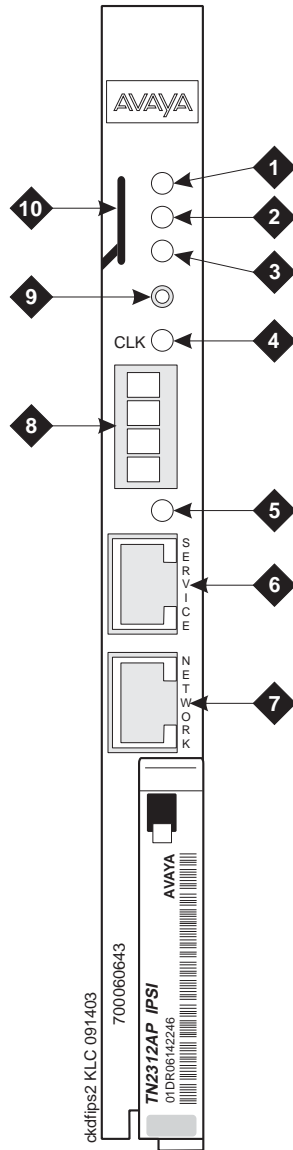
Figure notes

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

Figure 12: LED display on the IPSI circuit pack—static address
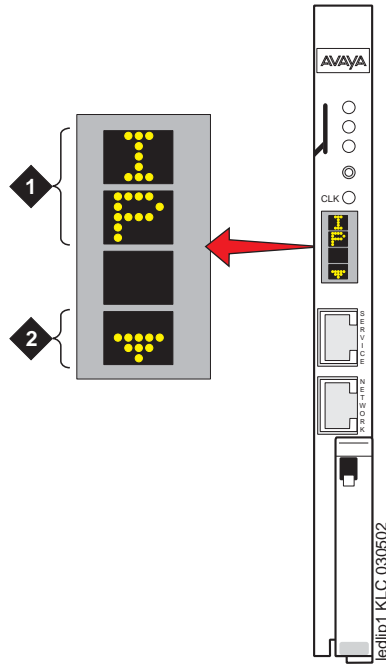
Figure notes

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

The display also indicates connectivity (see on page 80).

Figure 13: LED display indicating connectivity status—DHCP address
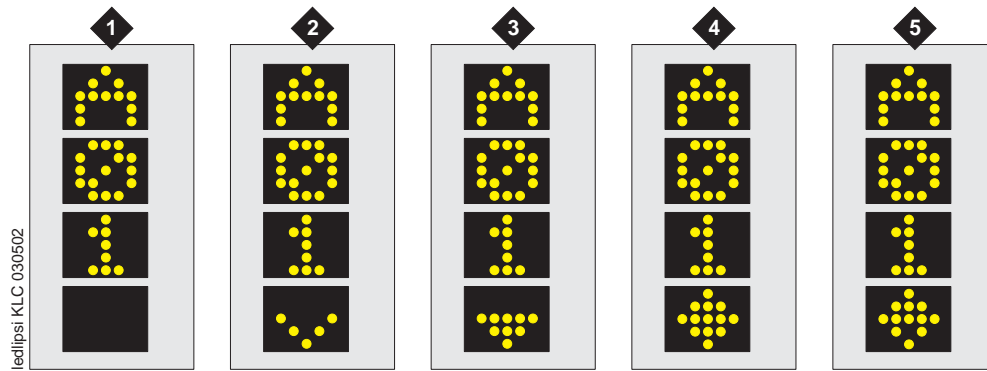
Figure notes

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

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 on page 81
- Connecting to the media server remotely over the network on page 84
- Connecting to the media server remotely over a modem on page 84
- Logins on page 86
- Network configuration on page 87

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 14, Services laptop computer connected directly to the S8700 Media Server, on page 82 or Figure 15, Services laptop computer connected directly to the S8710 Media Server, on page 83. 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 10/100 BaseT 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 87.

The network connection for the computer is

- IP address: 192.11.13.5

- Subnet mask: 255.255.255.252

Figure 14: Services laptop computer connected directly to the S8700 Media Server
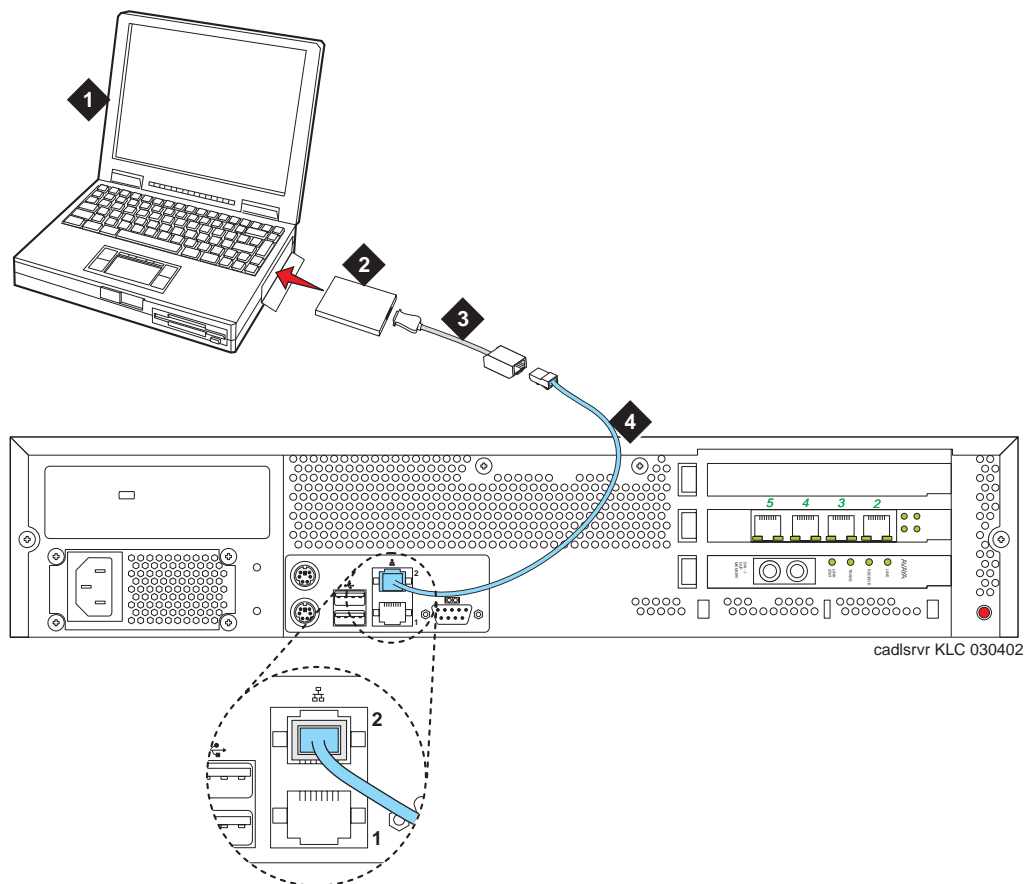
cadlsrvr KLC 030402

Figure notes

1	Services laptop	**3**	NIC adapter cable (if necessary)
2	Network Interface Card (NIC)	**4**	Black CAT5 crossconnect cable

Figure 15: Services laptop computer connected directly to the S8710 Media Server
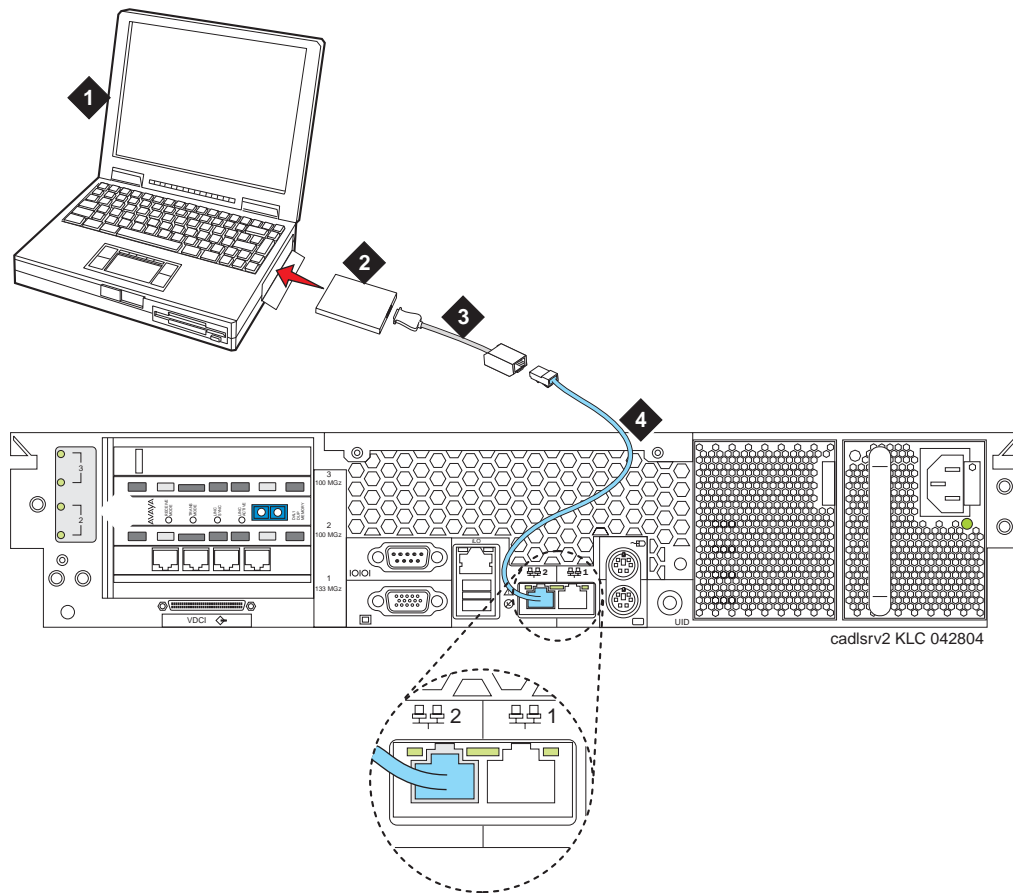
cadlsrv2 KLC 042804

Figure notes

1	Services laptop	**3**	NIC adapter cable (if necessary)
2	Network Interface Card (NIC)	**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 85 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.

You can also use the **active (alias)** media server address to connect automatically to the media server that is active.

Connecting to the media server remotely over a modem

This section covers the following tasks:

> **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.

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.

Finding the active media server IP address

1 To get the IP address of the actual active media server, go to the task bar at the bottom right of your PC screen.

2 Right-click on the Network Status icon, and select Status, then the Details tab.

3 Scroll down until you see the Server IP address. This is the IP address for the media server you are connected to.

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 14, Services laptop computer connected directly to the S8700 Media Server, on page 82 or Figure 15, Services laptop computer connected directly to the S8710 Media Server, on page 83) 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 88 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 use a command line interface in a Telnet window:

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 active media server. (SAT commands are usable only on the active 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:

- 9600 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 active media server using either the IP address or the DNS host name. Use port **5023** for this connection. (SAT commands are usable only on the active media server.) 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, assigned to the 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 Little Instruction Book for Basic Administration* (555-233-756) 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

> **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.

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 on page 89
- Configuring the media server hardware on page 90
- Installing the license and Avaya authentication files on page 91

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. - **S8700**: Open the door on the front of the media server and push the power button. - **S8710**: Push the power button on the front of the media server.
Servers are not shadowing	- Make sure you are using a crossconnect cable. - Make sure fiber optic cable is plugged in correctly. RX to TX and TX to RX.
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. - Make sure you are logged onto the active server.
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.
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**.

Problem	Solution
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.
Get "Anonymous memory" message when placing flashcard into PCMCIA drive	- **S8700**: Flashcard may be faulty; replace it.

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

H

hard drive
    remastering, 41
hardware
    connecting, 49
high-level overview of installation process, 25

I

inputing translations, 44
installation
    troubleshooting, 89
installation process
    high-level overview, 25
Installation Wizard
    using, 36
installing
    media gateways, 67
    software, 35
    translation file, 48
IP address
    set static, 51
    use DHCP, 50
IPSI
    administering, 45
    LEDs, 77
    program switch ID and cabinet, 50
    verify circuit pack version, 55
IPSI information
    adding, 45
IPSIs
    enabling control, 55
    verify translations, 54

K

keys, 11

L

LEDs
    alarms, 71
    Avaya P333T Ethernet switch, 76
    IPSI, 77
    S8700 Media Server, 71
    S8710 Media Server, 74
    testing on media server, 40
    testing on S8700 Media Server, 72
    UPS, 77
license file
    testing, 70

license status,verifying, 56
light emitting diodes. See LEDs.
location
    daylight savings rules, 59
    setting, 59

M

Maintenance Web Interface, accessing, 85
media gateways
    adding, 44
    installing, 67
media server
    accessing, 34
    backing up to compact flash media, 61
    configuring, 33, 43
    disconnecting from, 40
    LEDs, 71, 74
    powering up, 34
    registering, 66
    reset, 44
    telneting, 65
    testing LEDs, 40, 72
    verify connectivity, 55
media server 2
    configuring, 41
media server connection to LAN
    verifying, 38
modem
    access to media server, 84
    configuring, 39
    connect to media server
        collocated, 24
            separated servers, 24

P

PCMCIA drive
    backing up file to, 63
    on S8700 Media Server, 63
PCMCIA flashcard
    backing up files to, 63
powering up media server, 34
pre-installation information, 16

R

registering media server, 66
remastering the hard drive, 41
remote access to media server
    over modem, 84
    over network, 84
required hardware, 20
reset media server, 44

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com